DEFENDO
INTERNET APPLIANCE SERVER

Benutzerhandbuch

LINOGATE
INTERNET TECHNOLOGIES

Stand 18.12.2002, V4.0-2-2

1. Inhaltsverzeichnis

1. Inhaltsverzeichnis 1-1

2. Vorwort 2-7

2.1. Hinweise 2-7
2.2. Warenzeichen 2-8

3. Leistungsbeschreibung 3-9

3.1. Hardware des DEFENDO 3-9
3.2. Konfiguration des DEFENDO 3-10
3.3. LAN / WAN Anbindung 3-10
3.4. Benutzerverwaltung 3-10
3.5. E-Mail-Server 3-11
3.6. Firewall 3-11
3.7. Proxy-Cache 3-11
3.8. Virenscan 3-12
3.9. RAS-Anbindung 3-12
3.10. VPN-Server 3-12
3.11. DNS-Server 3-13
3.12. Web/FTP-Server 3-13
3.13. DHCP-Server 3-13

4. Vorsichtsmaßnahmen und Hinweise 4-14

4.1. Warnung 4-14
4.2. Zu Ihrer Sicherheit 4-14
4.3. Netzstecker 4-14
4.4. Aufstellungsort 4-14
4.5. Standard-Passwort 4-15

5. Anschließen des Gerätes 5-16

5.1. Auspacken 5-16
5.2. Mitgeliefertes Zubehör 5-16
5.3. Herstellen der Verbindungen 5-17
5.3.1. Anschluss an ISDN-Wählleitung (falls vorh.) 5-17
5.3.2. Anschluss an ISDN-Standleitung (falls vorh.) 5-17
5.3.3. Anschluss an xDSL-Wählverbindung (falls vorh.) 5-18
5.3.4. Anschluss an externen Router / xDSL-Standverbindung (falls vorh.) 5-18
5.3.5. Verbinden mit lokalem LAN (Netzwerk) 5-19
5.3.6. Anschluss ans Stromnetz 5-20

6. Einstellungen für die Inbetriebnahme 6-21
6.1. Vorausetzungen 6-21
6.2. Internet-Browser 6-21
6.3. TCP/IP-Protokoll und Einstellungen 6-21
6.4. Einschalten und Booten des DEFENDO 6-22
6.5. Einstellen der IP-Adresse 6-23
6.5.1. IP-Adress-Vergabe mit Hilfe des Displays 6-23
6.5.2. IP-Adress-Vergabe über die DEFENDO Konsole 6-23
6.5.3. IP-Adress-Vergabe durch umkonfigurierten PC 6-24
6.5.4. Überprüfung der Verbindung zum DEFENDO 6-27
6.5.5. Starten der WEB-Oberfläche des DEFENDO 6-28
6.5.6. Erste Einstellungen des DEFENDO 6-30
7. Das Hauptmenü „Konfiguration“ 7-31
7.1. Der Konfigurations-Assistent „LAN-Anbindung“ 7-31
7.1.1. Vergabe der IP-Adresse des DEFENDO 7-33
7.1.2. Vergabe des Domänen-Namens Ihres LANs 7-34
7.1.3. IP-Adressen des internen LANs definieren 7-35
7.1.4. Der DHCP-Dienst des DEFENDO 7-36
7.1.4.1. Verwenden des sekundären DHCP-Dienstes 7-37
7.1.4.2. Verwenden des primären DHCP-Dienstes 7-38
7.1.5. LAN-Anbindung fertigstellen 7-39
7.2. Der Konfigurations-Assistent „Fernwartung“ 7-40
7.2.1. Einrichten des Protokolls und der MSN/EAZ 7-42
7.2.2. Einrichtung für den Support (ausgehend) 7-43
7.2.3. Einrichtung für den Support (eingehend) 7-44
7.2.4. Callback-Funktion einrichten 7-45
7.3. Der Konfigurations-Assistent „Internet-Zugang“ 7-47
7.3.1. Internetanbindung mit ISDN-Wählleitung 7-48
7.3.2. Internetanbindung mit ADSL-Wählleitung 7-49
7.3.3. Internetanbindung über Ethernet-Router 7-50
7.3.4. Internet-Zugang über „andere Provider“ 7-53
7.3.4.1. Einwahldaten eingeben 7-53
7.3.4.2. Der DNS-Server Ihre Providers 7-54
7.3.4.3. Der Proxy-Cache-Server des Providers 7-55
7.3.4.4. Mailserver des Providers 7-57
7.3.5. Internet-Zugang über T-Online Wählleitungen 7-59
7.3.5.1. T-Online Zugangsdaten 7-60
7.3.5.2. E-Mail-Account über „eigene Domain“ 7-61
7.3.6. Internet-Zugang fertigstellen 7-62
7.4. Der Konfigurations-Assistent „eMail-Einrichtung“ 7-62
7.4.1. DEFENDO ist selbst Mail-Server für Ihr LAN 7-63
7.4.1.1. Mail Domains eintragen 7-64

7.4.1.2. Virenscanner aktivieren 7-65
7.4.1.3. POP3-Server bearbeiten 7-65
7.4.1.4. Neuen POP3-Server anlegen 7-66
7.4.1.5. Bestehenden POP3-Server bearbeiten 7-67
7.4.1.6. Postfächer bearbeiten 7-68
7.4.1.7. Hinzufügen eines Postfaches 7-69
7.4.1.8. Postfächer über Einzelkonto 7-72
7.4.1.9. Postfächer über Sammelkonto 7-73
7.4.2. DEFENDO stellt Mails an einen anderen Mail-Server im LAN zu 7-75
7.4.2.1. Angabe des internen Mail-Servers 7-75
7.4.2.2. Die Domains des internen Mail-Servers 7-76
7.4.3. Weitere Optionen unter eMail-Einrichtung 7-77
7.4.3.1. POP3-Server mit allen Postfächern löschen 7-77
7.4.3.2. Zustellungs- und Abholzeiten für Mails 7-78
7.4.3.2.1. Versenden von Mails über Standleitung 7-79
7.4.3.2.2. Versenden von Mails über Wählleitung 7-80
7.4.3.2.3. Abholzeiten für POP3-Mails 7-81

8. Einstellungen der LAN-PCs fürs Internet 8-83

8.1. Verwendung eines DHCP-Servers 8-83
8.2. Einstellungen am lokalen PC 8-83
8.3. Einrichten des Browers 8-85

9. Das Hauptmenü „Administration“ 9-89

9.1. Grundeinstellungen 9-89
9.2. Benutzer 9-90
9.2.1. Allgemeine Hinweise zu Benutzern 9-90
9.2.2. Aufnahme / Ändern von Benutzern 9-92
9.2.2.1. Einstellungen für die Gruppe system-mail 9-93
9.2.2.2. Einstellungen für die Gruppe system-proxy 9-95
9.2.2.3. Einstellungen für die Gruppe system-web 9-96
9.2.2.4. Passwortoptionen für Benutzer 9-96
9.2.2.5. Benutzer löschen / Übernehmen 9-97
9.2.3. Hinweis zum Benutzer „admin“ 9-97
9.3. Gruppen 9-97
9.3.1. Allgemeine Hinweise zu Gruppen 9-97
9.3.2. Aufnahme / Ändern von Gruppen 9-98
9.3.2.1. Sonderbedeutung der Gruppe system-mail 9-100
9.3.2.2. Sonderbedeutung der Gruppe system-proxy 9-101
9.4. Proxylisten 9-101
9.4.1. Allgemeines zu Proxylisten 9-101
9.4.2. Anlegen / Ändern von Proxylisten 9-102
9.4.3. Proxyliste konfigurieren 9-104
9.4.4. Hinweis zu den Datenbankkategorien 9-106

9.5. Zertifikate 9-106
9.5.1. Neues HTTPS-Server Zertifikat 9-107
9.5.2. Neues Mail-Server Zertifikat 9-107
9.5.3. Neues VPN-Server Zertifikat 9-108
9.5.4. VPN-Server-Zertifikat exportieren 9-108
9.6. Backup 9-109
9.6.1. Einstellungen zurückschreiben 9-109
9.6.2. Auslieferungskonfiguration wiederherstellen 9-111
9.6.3. Sichern der Konfiguration 9-111
9.7. Update 9-115
9.8. Neustart 9-117
9.9. Lizenzen 9-118

10. Das Hauptmenü „Home“ 10-120

10.1. Benutzer 10-120
10.1.1. Passwort ändern 10-121
10.1.2. Weiterleiten von E-Mails 10-122
10.1.3. Webmail 10-123
10.2. Produktpass 10-124
10.3. Systemstatus 10-125
10.4. Abmelden 10-126
10.5. Kontakt 10-126

11. Das Hauptmenü „Monitoring“ 11-128

11.1. Dienste 11-128
11.1.1. Automatisches Starten von Diensten 11-129
11.1.2. Sofortbefehle für Dienste 11-129
11.1.3. Der Dienst „Ethernet“ 11-130
11.1.4. Der Dienst „ISDN“ 11-130
11.1.5. Der Dienst „ADSL / PPP over Ethernet“ 11-131
11.1.6. Der Dienst VPN / IPSec 11-131
11.1.7. Der Dienst „Firewall“ 11-131
11.1.8. Der Dienst „dynamische Firewall“ 11-131
11.1.9. Der Dienst „Intrusion Detection“ 11-131
11.1.10. Der Dienst „DHCP-Server“ 11-132
11.1.11. Der Dienst „DNS-Server“ 11-132
11.1.12. Der Dienst „Proxy-Cache“ 11-132
11.1.13. Der Dienst „Mail-Server“ 11-132
11.1.14. Der Dienst „POP3 / FTP“ 11-132
11.1.15. Der Dienst „HTTP-Server“ 11-133
11.1.16. Der Dienst „DEFENDO -Konfiguration“ 11-133
11.1.17. Der Dienst „Windows-Freigaben“ 11-133
11.1.18. Der Dienst „Zeitsteuerung“ 11-133
11.1.19. Der Dienst „System-Logging“ 11-133

11.2. Log-Dateien ... 11-134
11.2.1. Log-Dateien archivieren ... 11-135
11.2.2. Log-Dateien anzeigen ... 11-137
11.2.3. Erweiterte Suchoptionen ... 11-138
11.2.4. Besonderheiten bestimmter Log-Dateien ... 11-139
11.2.4.1. Meldungen – nur Firewall ... 11-139
11.2.4.2. Meldungen – nur DNS-Anfragen ... 11-140
11.2.4.3. Meldungen - nur ISDN-Leitungsstatus ... 11-141
11.2.4.4. wichtige Meldungen – nur Intrusion Detection ... 11-143
11.3. Systeminfo ... 11-143
11.4. Mail-Server ... 11-144
11.5. ISDN ... 11-146
11.6. Verbindung ... 11-148
11.7. Last-Statistik ... 11-149
11.8. Netzwerk-Statistik ... 11-150
11.9. Proxy-Statistik ... 11-151
11.10. Web-Statistik ... 11-153

12. Das Hauptmenü „Expertenmodus“ ... 12-155

12.1. Schnittstellen ... 12-155
12.1.1. Ethernet ... 12-158
12.1.2. ISDN syncPPP ... 12-160
12.1.3. ISDN HDLC-RawIP ... 12-165
12.1.4. ADSL / PPP over Ethernet ... 12-169
12.1.5. Serielles Modem ... 12-171
12.1.6. VPN ... 12-172
12.1.6.1. Die VPN-Hauptmaske ... 12-173
12.1.6.2. Verbindung zu VPN-Servern mit fester IP ... 12-175
12.1.6.3. Verbindung zu VPN-Servern mit dynamischer IP ... 12-178
12.1.6.4. X.509-Zertifikat festlegen ... 12-180
12.2. Firewall ... 12-183
12.2.1. Die Firewall-Hauptmaske ... 12-184
12.2.2. Die Firewall-Schnittstellen Maske ... 12-188
12.2.2.1. Vertrauen nicht definiert – Schnittstelle blockiert ... 12-190
12.2.2.2. Vertrauen keines (Internet) ... 12-191
12.2.2.3. Vertrauen gering (Demilitarisierte Zone) ... 12-199
12.2.2.4. Vertrauen mittel (RAS) ... 12-201
12.2.2.5. Vertrauen hoch (LAN) ... 12-202
12.2.2.6. Vertrauen Fernwartung ... 12-203
12.3. DHCP ... 12-203
12.4. DNS ... 12-206
12.4.1. Verwaltete Domains ... 12-208
12.4.2. Verwaltete IP-Adressbereiche ... 12-211
12.5. Proxy-Cache ... 12-214

12.6. Mail-Server 12-223
12.7. Mail-Client 12-230
12.7.1. Mail-Client Einträge bearbeiten (POP3) 12-232
12.7.2. Mail-Client Einträge bearbeiten (ETRN) 12-235
12.8. Http-Server 12-236
12.9. FTP-Server 12-238
12.10. Windows 12-239
12.11. Virenscanner 12-240
12.11.1. Installation Kaspersky Virenscanner 12-243
12.11.2. Installation McAfee Virenscanner 12-245
12.12. Zeit-Server 12-246

13. Kontakt 13-248

14. Support für Ihren DEFENDO 14-249

15. Technische Daten 15-250

16. CE-Konfirmitätserklärung 16-251

2. Vorwort

Wir bedanken uns, dass Sie sich für das Produkt Defendo entschieden haben.

Bei diesen Gerät handelt es sich um einen Router, Internet-Appliance-Server, Firewall und E-Mail-Server ... und das alles in einem Gerät! Natürlich bietet Ihnen der Defendo je nach Ausstattungsvariante noch eine ganze Reihe weitere Features. Damit Sie ihn auch optimal für Ihre Zwecke nützen und bedienen können, haben wir versucht dieses Installationshandbuch so einfach wie möglich zu gestalten. Deshalb nehmen Sie sich bitte die Zeit, dieses Handbuch sorgfältig zu lesen, da sich einige Abschnitte auf vorgelagerte Kapitel beziehen.

Da das Produkt Defendo ständig weiterentwickelt wird, empfehlen wir Ihnen den Erwerb eines Wartungsvertrages, der Sie kostenfrei mit Produkt-Updates und Upgrades, also auch neuen Funktionen versorgt. Auch sollten Sie sich unbedingt bei uns registrieren lassen, damit wir Ihnen schnell und unbürokratisch im Supportfalle helfen können.

Aufgrund der ständigen Verbesserung kann es vorkommen, dass bestimmte Bereiche in diesem Handbuch noch nicht vollständig beschrieben sind. In diesem Fall, bitten wir Sie, sich auf unserer Homepage www.defendo.de mit etwaigen hier fehlenden Informationen zu versorgen.

Sollten doch Probleme bei der Konfiguration des Gerätes auftreten, die Sie nicht alleine lösen können, steht Ihnen selbstverständlich unter den bekannten Supportnummern fachlich versierte Hilfe zur Verfügung. Alle Angaben zum Kontakt mit ihm erhalten Sie im Kapitel 14.

2.1. Hinweise

Dieses Handbuch wurde mit größtmöglicher Sorgfalt und Genauigkeit erstellt. Trotzdem kann von der LINOGATE GmbH keinerlei Gewähr sowie Haftung auf Vollständigkeit und fehlerfreien Inhalt gegeben bzw. übernommen werden.

Da dieses Gerät die Funktionalität eines Routers beinhaltet, ist darauf zu achten, dass alle Einstellungen im Erstbetrieb überwacht und geprüft werden. Verwenden Sie hierzu z.B. den ISDN-Monitor, wie im Kapitel 11.5 beschrieben. Ein falsch konfiguriertes Gerät kann erhebliche Verbindungskosten zur Folge haben, für die wir keine Verantwortung übernehmen können.

Dieses Handbuch beschreibt alle Versionen des DEFENDO. Bitte beachten Sie, dass je nach erworbener Version die Funktionalität unterschiedlich ist. Fehlt bei Ihrem Gerät Funktionalität, die in diesem Handbuch beschrieben ist, so können Sie diese nachordern, sofern es die Software betrifft. Bitte fragen Sie sich in diesem Fall an Ihren Vertriebspartner (siehe Kapitel 13). Je nach Ausstattung der Hardware können ebenfalls einige Funktionen nicht verwendet werden. Ihr Vertriebspartner wird Ihnen auch hier sicher Lösungsmöglichkeiten aufzeigen.

Technische Änderungen des Gerätes sind ohne vorherige Ankündigung vorbehalten.

2.2. Warenzeichen

Alle hier genannten Firmen- und Produktbezeichnungen sind eingetragene Warenzeichen des jeweiligen Inhabers. DEFENDO ist ein eingetragenes Warenzeichen der LINOGATE GmbH. Die Nennung hier nicht aufgeführter Warenzeichen ist kein Hinweis auf deren freie Verfügbarkeit.

Copyright ©, LINOGATE GmbH

3. Leistungsbeschreibung

Mit der vorliegenden Version des DEFENDO erhalten Sie einen leistungsfähigen Internet-Appliance-Server, der viele Funktionen für die Kommunikation im Internet und dessen Möglichkeiten in einem Gerät vereint. Natürlich sind auch Sicherheitsmechanismen wie ein effizientes Firewallsystem oder die Verschlüsselung von Verbindungen (Virtuell Privat Network) integriert, bzw. als Option erhältlich. Zusätzliche teure Softwareprodukte, die auf Netzwerkbetriebssystemen wie Microsoft Windows NT 4.0 Server oder Windows 2000 Server sowie Novell Netware 3.x, 4.x oder 5.x aufgesetzt werden müssen, sind somit nicht mehr notwendig. Meist sind diese Produkte gar nicht ohne weitere Hardware oder Aufrüstung der bestehenden Hardware vernünftig einzusetzen.

Hinweis:

Die Spezifikationen sowie Verfügbarkeit von Funktionen können je nach Variante des Gerätes unterschiedlich sein. Zur Erweiterung des DEFENDO wenden Sie sich bitte an den technischen Support (siehe Kapitel 14).

3.1. Hardware des DEFENDO

In allen Geräten wird ein Intel Celeron Prozessor mit mindestens 1 GHz, sowie mindestens 128 MB RAM verwendet. Die Netzwerkanbindung erfolgt über zwei 10/100 Mbit Netzwerkkarten. Ein BNC-Anschluß ist nicht verfügbar. Für die ISDN-Anbindung ist ein ISDN-Adapter integriert. Zur Aufnahme der Betriebsystem-Software sowie der Daten für Proxy-Cache, E-Mails usw. wurde eine Festplatte mit mindestens 10 GB Kapazität vorgesehen. Je nach Variante (DEFENDO small, medium oder large) und Ausstattung kann auch ein 19“-Gehäuse, 256 MB RAM und eine Software-Plattenspiegelung zur Verfügung sein.

3.2. Konfiguration des DEFENDO

Der DEFENDO kann mit Hilfe eines Internet-Browsers webbasierend konfiguriert werden. Alle Zugriffe bei der Administration von der Workstation zum DEFENDO können verschlüsselt übertragen werden. Sollte eine Fernwartung durch den Support (siehe Kapitel 14) gewünscht oder notwendig sein, so ist diese ebenfalls verschlüsselt. Diese kann über direkte Einwahl (RAS) oder über das Internet erfolgen. Alle Neuerungen bzw. Updates können vom Internet heruntergeladen und dann eingespielt werden. Alle Einstellungen wie Konfiguration (IP-Adresse, Provider-Daten, etc.) können als Datei auf eine beliebige Festplatte oder Diskette gespeichert werden. Das Gleiche gilt für Benutzer-Daten und deren Passwörter.

3.3. LAN / WAN Anbindung

Es stehen mehrere Möglichkeiten zur Verfügung, den DEFENDO ans WAN anzubinden. Hierbei werden ISDN-Wählleitungen mit 64 kbits oder 128 kbits über das D-Kanal Protokoll EDSS1, 1TR6 oder NI1 unterstützt. Als Verbindungs-Protokoll können syncPPP oder HDLC eingesetzt werden. ISDN-Standleitungen (64S1 oder 64S2 mit den Protokollen syncPPP oder HDLC) können zum Einsatz kommen. Auch an ADSL/T-DSL-Anschlüsse (PPP over Ethernet) kann ein Anschluss realisiert werden. Wenden Sie sich im Zweifelsfalle an den technischen Support (siehe Kapitel 14). Internet-Verbindungen über PPP können bezüglich Einwahldauer und –häufigkeit überwacht werden.

Eine Anbindung rein über Ethernet ist mit Hilfe eines externen Routers möglich. Auf der Clientseite können beliebige Clients mit TCP/IP-Unterstützung über Ethernet angebunden werden.

3.4. Benutzerverwaltung

Mit Hilfe der Benutzerverwaltung ist es möglich, bei einer Internetanfrage eines Benutzers seine Kennung und sein Passwort (über den integrierten Proxy-Cache-Server) abzufragen. Alle Zugriffe werden dabei exakt protokolliert. Auch kann eingestellt werden, auf welche Dienste der Benutzer im DEFENDO zugreifen darf. Für die benutzerspezifisch freigeschalteten Dienste können unterschiedliche Passwörter vergeben werden.

3.5. E-Mail-Server

Ausgehende E-Mails werden mit SMTP unterstützt. Für eingehende E-Mails kann zwischen SMTP, ETRN oder POP3 ausgewählt werden. Es werden zudem POP3-Multi-Drop Mailbox-Konten unterstützt. Alle Mails können auf ihre maximale Größe eingestellt werden. Der DEFENDO kann für weitere Mail-Server als Mail-Gateway verwendet werden. Unbekannte Mail-Empfänger können in einem „Zentraleingang“ abgelegt werden. Eine Verteilung und Weiterleitung von E-Mails ist integriert und kann zum Teil durch die Benutzer selbst verwaltet werden. Der verfügbare POP3/IMAP4-Server erlaubt den Zugriff von Standard-Mail-Clients (z. B. MS-Outlook).

3.6. Firewall

Der Firewall basiert auf einem stateful inspection IP-Filter. Eine Network-Adress-Translation (NAT) ist integriert und kann individuell eingestellt werden. Die Intrusion Detection erkennt Angriffe innerhalb der Datenströme sowie eventuell bereits befallene Systeme. Die dynamische Firewall erkennt bestimmte Angriffsmuster und kann individuell reagieren.

3.7. Proxy-Cache

Das Caching von Web-Seiten kann eingestellt werden. Ein Proxy für die Dienste http, https, ftp, gopher und wais steht zur Verfügung. Die aktivierbare Passwortabfrage beim Internetzugriff ermöglicht benutzerbezogen konfigurierbaren Internetzugriff und Protokollierung. Zudem können Zeit- und Mengenkontingenten für jeden Benutzer zugeteilt werden. Eine Statistik des gesamten Datenverkehrs wird generiert. Eine Download-Sperrung von definierbaren Datei-Endungen ist möglich, sowie die Einschränkung des Zugriffes auf definierbare URLs. Auch können aktive HTML-Inhalte ausgeblendet werden.

3.8. Virenscan

Hinweis:

Zur Verwendung dieser Option ist der Erwerb einer Virenscanner-Lizenz unbedingt notwendig. Die Lizenz ist im Lieferumfang nicht enthalten. Unterstützte Virenscanner sind der „Kaspersky Anti-Virus for Appliance-Server“ sowie der McAfee Command-Line Virenscanner für Linux in Version 4.x der unter anderem in den Produktpaketen „Total Virus Defense Suite“ oder „Virus Scan Security Suite“ enthalten ist.

Den DEFENDO Mail-Server passierende E-Mails sowie Datei-Downloads über den Proxy-Cache des DEFENDO können automatisch auf Viren überprüft werden. Die Virensignatur-Datenbanken der Virenscanner lassen sich intervall-gesteuert automatisch vom DEFENDO aus dem Internet herunterladen. Diese Signaturen können auch für andere Server und Clients im LAN bereitgestellt werden.

3.9. RAS-Anbindung

Zur Anbindung von Außenstellen oder Home-Office-Arbeitsplätzen wird ein AsyncPPP-Protokoll über serielles Analog- oder ISDN-Modem unterstützt, sowie ISDN-Wählleitungen mit 64kbit/s und SyncPPP- oder HDLC-Protokoll. RAS-PCs können in das LAN mit Hilfe von ProxyARP eingebunden werden. Unterstützt wird auch die Einbindungen kompletter Netzwerke über TCP/IP-Routing.

3.10. VPN-Server

Der verfügbare VPN-Server oritentiert sich weitgehend am IPSEC-Standard und unterstützt Tunnel- und Transport-Mode. Als Verschlüsselungsalgorithmus steht ausschließlich TripleDES zur Verfügung, während an Hashfunktionen sowohl SHA als auch MD5 unterstützt werden. Die Authentifizierung erfolgt über Preshared Key oder X.509-Zertifikate. Für Perfect-Forward-Secrecy sind die Diffie-Hellman Gruppen 2 und 5 verfügbar.

3.11. DNS-Server

Konfigurierbare Einträge erlauben den Einsatz als Caching-DNS-Servers im LAN.

3.12. Web/FTP-Server

Der verfügbare Apache Web-Server kann als Intranet- und / oder Internet-Web-Server eingesetzt werden. Er beinhaltet eine CGI-Unterstützung. Die Verwaltung des Web-Server kann über FTP oder Windows-Freigaben erfolgen. Der anonymous FTP-Server besitzt eine Upload-Möglichkeit.

3.13. DHCP-Server

Es besteht die Möglichkeit, den DEFENDO als „Primary“ oder „Secondary“ DHCP-Server im LAN mit Hilfe konfigurierbare Adressbereiche einzusetzen.

4. Vorsichtsmaßnahmen und Hinweise

Bitte lesen Sie die nachfolgenden Abschnitte aufmerksam durch, bevor Sie den DEFENDO in Betrieb nehmen.

4.1. Warnung

Zur Verhütung von Brand und elektrischem Schlag darf dieses Gerät weder Regen noch Nässe ausgesetzt werden.

4.2. Zu Ihrer Sicherheit

Auf keinen Fall das Gehäuse öffnen oder sogar im offenen Zustand betreiben, da die Gefahr von elektrischem Schlag besteht. Zudem können schwere Geräteschäden verursacht werden. Im Inneren des Gerätes befinden sich keine Teile, die vom Nichtfachmann gewartet werden können. Bitte wenden Sie sich für Geräteerweiterungen oder Reparaturen nur an den Kundendienst.

4.3. Netzstecker

Unterlassen Sie das Anschließen des Netzsteckers mit feuchten oder gar nassen Händen. Halten Sie das Netzkabel von Heizquellen fern. Stellen Sie keine schweren Gegenstände auf das Netzkabel. Falls das Gerät Rauch, ungewöhnliche Gerüche oder Geräusche abgibt, ziehen Sie unverzüglich den Netzstecker ab und setzen Sie sich mit dem Kundendienst in Verbindung.

4.4. Aufstellungsort

Vermeiden Sie ein Aufstellen in direkter Sonneneinstrahlung, neben Heizgeräten, an Orten mit hohen Temperaturen (mehr als 35°C) oder hoher Feuchtigkeit (mehr als 90%) und sehr staubigen Orten. Stellen Sie das Gerät nicht an Plätzen auf, an denen es Vibrationen ausgesetzt sein könnte. Verwenden Sie nur eine ebene Fläche zum Aufstellen, da sonst Bauteile im Inneren beschädigt werden können. Halten Sie das

Gerät auch fern von magnetischen Gegenständen bzw. Gegenständen, die Magnete enthalten, z. B. Lautsprecher-Boxen.

4.5. Standard-Passwort

Zur Konfiguration des Gerätes sind administrative Rechte notwendig. Zu diesem Zweck wurde ein Administrator-Benutzer und ein Passwort vergeben. Zu Ihrer Sicherheit sollte das Passwort sofort nach der Grundeinrichtung geändert werden. Bei entsprechender Abfrage nach Benutzer und Kennwort verwenden Sie bitte als Benutzer „**admin**“ und als Kennwort „**redhat**“. Bitte achten Sie auf die Schreibweise wie hier angegeben, da das eingesetzte Betriebssystem Groß- und Kleinschreibung unterscheidet.

Hinweis:

Bitte ändern Sie wie ab Kapitel 10.1.1 beschrieben das Standard-Passwort auf Ihr gewünschtes Passwort. Dies ist für Ihre Sicherheit unbedingt notwendig, da diese Beschreibung auch in Hände gelangen kann, die sich fremden Zugriff auf den DEFENDO verschaffen wollen.

5. Anschließen des Gerätes

5.1. Auspacken

Entnehmen Sie das Gerät vorsichtig aus der Verpackung. Bewahren Sie den Karton mit allen Verpackungsmaterialien für einen späteren Versand oder Transport auf. Sollte das Gerät starken Temperaturschwankungen ausgesetzt gewesen sein (z. B. vom kalten Fahrzeug in einen geheizten Raum), warten Sie cirka 1 Stunde ab, damit es sich klimatisieren kann. Dies ist ratsam, da sich Kondensation im Gerät gebildet haben könnte, die beim Einschalten schwere Geräteschäden verursachen kann.

5.2. Mitgeliefertes Zubehör

Überprüfen Sie den Verpackungsinhalt anhand der folgenden Liste. Sollten Teile fehlen, so wenden Sie sich bitte umgehend an ihren Fachhändler.

- DEFENDO (Internet Appliance Server)
- pro ISDN-Anschluß je ein ISDN-Kabel (schwarz)
- pro Netzwerkanschluß je ein Netzwerkkabel (grau), TP, CAT 5+
- Stromanschlußkabel (Schuko-Kaltgerätekabel)
- CD mit Installationsprogramm und Handbuch als PDF
- Kurzanleitung

5.3. Herstellen der Verbindungen

5.3.1. Anschluss an ISDN-Wählleitung (falls vorh.)

Von diesem Gerät unterstützt werden folgende Wähleitungs-verfahren:

- S0-Bus Punkt-zu-Mehrpunkt (Mehrgeräte) Anschluß
- 64 kbits/s oder 128 kbits/s
- EDSS1 oder 1TR6
- syncPPP oder HDLC

Stecken Sie das mitgelieferte ISDN-Kabel in den vorhandenen ISDN-NTBA oder an einen bereitgestellten S0-ISDN-Anschluss (WAN) Ihrer Telefonanlage. Verbinden Sie das Gegenstück des Kabels mit dem als „ISDN“ gekennzeichneten Anschluss auf der Rückseite des Gerätes.

> *Hinweis:*
>
> *Achten Sie unbedingt darauf, dass es sich wirklich um die ISDN-Buchse handelt! Ein Verwechseln mit dem Netzwerkanschluss des Gerätes kann schwere Geräteschäden hervorrufen!*

Sollte das Gerät über mehrere ISDN-Adapter verfügen, so wiederholen Sie den Vorgang entsprechend. Vergewissern Sie sich beim Betrieb an einer Telefonanlage, dass diese sämtliche Dienstmerkmale auch weitergibt. Ein Betrieb an einem analogen Anschluss ist nicht möglich.

5.3.2. Anschluss an ISDN-Standleitung (falls vorh.)

Von diesem Gerät unterstützt werden folgende Standleitungsverfahren:

- 64S1 oder 64S2
- syncPPP oder HDLC

Stecken Sie das mitgelieferte ISDN-Kabel in den vorhandenen ISDN-NTBA. Verbinden Sie das Gegenstück des Kabels mit dem als ISDN-

Buchse gekennzeichneten Anschluss (WAN) auf der Rückseite des Gerätes.

> *Hinweis:*
>
> *Achten Sie unbedingt darauf, dass es sich wirklich um die ISDN-Buchse handelt! Ein Verwechseln mit dem Netzwerkanschluss des Gerätes kann schwere Geräteschäden hervorrufen!*

5.3.3. Anschluss an xDSL-Wählverbindung (falls vorh.)

Von diesem Gerät unterstützt werden folgende xDSL-Leitungsverfahren:

- ADSL / T-DSL (PPP over Ethernet)

In diesem Fall sind 2 Netzwerkkarten im DEFENDO notwendig. Das zweite Kabel dient zur Anbindung an das LAN. Es muss somit an Ihren vorhanden Hub oder Switch und mit der als LAN gekennzeichneten Buchse auf der Rückseite des DEFENDO angeschlossen werden. Stecken Sie das mitgelieferte Netzwerkkabel in das bereitgestellte xDSL-Modem Ihres Providers. Verbinden Sie das Gegenstück des Kabels mit dem verbleibenden Anschluss (nicht ISDN) auf der Rückseite des Gerätes.

> *Hinweis:*
>
> *Achten Sie unbedingt darauf, dass Sie die Buchsen nicht vertauschen! Ein Verwechseln kann dazu führen, dass der DEFENDO nicht ansprechbar ist!*

5.3.4. Anschluss an externen Router / xDSL-Standverbindung (falls vorh.)

Von diesem Gerät wird ein 10/100 Mbit Anschluss über Hub oder Switch unterstützt.

Sollten Sie das Gerät in einer Bus-Verkabelung (BNC) betreiben wollen, so benötigen Sie einen optional erhältlichen Media-Konverter (BNC auf

Twisted Pair, z. B. Allied Telesyn). Wenden Sie sich in diesem Falle an Ihren Support (siehe Kapitel 14).

Verbinden Sie das mitgelieferte Patchkabel mit einem freien Anschluss eines Hubs oder Switches, der mit dem externen Router verbunden ist. Verwenden Sie dazu nicht den Hub oder Switch, über den auch das LAN angeschlossen ist, sondern ein eigenes Gerät. Das andere Ende des Patchkabels stecken Sie bitte in den als Netzwerkanschluss, der nicht als ISDN Anschluss gekennzeichnet ist.

Dieses Gerät kann auch direkt an den externen Router angeschlossen werden, wenn dieser über einen passenden Ethernet-Anschluss verfügt. Verwenden Sie hierzu ein *gedrehtes* Patchkabel. Verbinden Sie den DEFENDO in diesem Fall direkt mit dem Netzwerk-Anschluss des Routers.

> *Hinweis:*
>
> *Achten Sie unbedingt darauf, dass es sich wirklich um die Netzwerk-Buchse handelt! Ein Verwechseln mit dem ISDN-Anschluss des Gerätes kann schwere Geräteschäden hervorrufen!*

5.3.5. Verbinden mit lokalem LAN (Netzwerk)

Von diesem Gerät wird ein 10/100 Mbit Anschluss über Hub oder Switch unterstützt.

Sollten Sie das Gerät in einer Bus-Verkabelung (BNC) betreiben wollen, so benötigen Sie einen optional erhältlichen Media-Konverter (BNC auf Twisted Pair, z. B. Allied Telesyn). Wenden Sie sich in diesem Falle an Ihren Support (siehe Kapitel 14).

Verbinden Sie das mitgelieferte Patchkabel mit einem freien Anschluss Ihres Hubs oder Switches. Das Gegenstück stecken Sie bitte in den als Netzwerkbuchse gekennzeichneten Anschluss auf der Rückseite des Gerätes. Ausnahmen hierbei sind zu berücksichtigen, wenn der DEFENDO über 2 Netzwerkkarten verfügt (z. B. beim Betrieb an xDSL-Anschlüssen).

Dieses Gerät kann auch direkt nur an einem PC angeschlossen werden, wenn dieser über eine Netzwerkkarte verfügt. Verwenden Sie hierzu ein *gedrehtes* Patchkabel. Verbinden Sie den DEFENDO in diesem Fall direkt mit der Netzwerkkarte des PCs.

Hinweis:

Achten Sie unbedingt darauf, dass es sich wirklich um die Netzwerk-Buchse handelt! Ein Verwechseln mit dem ISDN-Anschluss des Gerätes kann schwere Geräteschäden hervorrufen!

5.3.6. Anschluss ans Stromnetz

Vergewissern Sie sich, dass der Netzschalter auf der Rückseite des Gerätes auf der Position „0“ steht.

Verwenden Sie zum Anschluss das mitgelieferte Netzkabel. Bitte beachten Sie, dass ein Betrieb des Gerätes nur an einem 230 Volt Wechselstromkreislauf möglich ist.

Es ist empfehlenswert, das Gerät an einer USV (Unterbrechungsfreie Stromversorgung) anzuschließen. Bei plötzlichem Stromausfall kann die Konfiguration des DEFENDO oder gar Hardwarebauteile beschädigt werden.

6. Einstellungen für die Inbetriebnahme

6.1. Vorausetzungen

Um die notwendigen Einstellungen des DEFENDO vornehmen zu können, benötigen Sie einen PC, der über eine Netzwerkkarte verfügt und entsprechend mit dem DEFENDO verbunden ist. Da Microsoft Windows 9x das meist installierte Betriebssystem auf dem Markt ist, sind alle nachfolgenden Installationshinweise darauf aufbauend. Es gelten nur geringe Abweichungen zum Betriebssystem Windows NT 4.0 Workstation, die bei der Konfiguration des DEFENDO eine Rolle spielen. Auf diese wird entsprechend hingewiesen.

6.2. Internet-Browser

Da alle Einstellungen des DEFENDO über eine graphische Benutzeroberfläche eingestellt werden können, muss auf diesem PC ein Internet-Browser installiert sein. Hierbei kann z. B. der Microsoft Internet Explorer ab Version 4.x eingesetzt werden oder der Netscape Navigator ab Version 3.x.

6.3. TCP/IP-Protokoll und Einstellungen

Bei der Netzwerkkarte ist zu beachten, dass das TCP/IP-Protokoll installiert sein muss. Sollte dies nicht der Fall sein, so lesen Sie bitte die notwendigen Schritte zur Installation des TCP/IP-Protokolls im Handbuch Ihres Betriebssystems bzw. Netzwerkbetriebsystems nach.

Hinweis:

Sie dürfen IP-Adressen für Ihr LAN nicht einfach erfinden. Gemäß Internetstandard RFC-1918 sind für lokale Netzwerke alle Adressen vorgesehen, die mit 10, mit 172.16 bis 172.31 und mit 192.168 beginnen. Alle IP-Adresse außerhalb der privaten Subnetze sind im Internet offiziell vergeben und das Eigentum von Firmen. Es empfiehlt sich daher dringend, für das interne LAN nur diese privaten Subnetze zu verwenden. Verwenden Sie also z.B. das Netzwerk „192.168.0.0“ mit der Netzmaske „255.255.255.0“. Sie können dann 254 IP-Adressen im Bereich 192.168.0.1 bis 192.168.0.254 in Ihrem LAN vergeben. Jede IP-Adresse darf nur einmal im Netzwerk vorkommen. Alle Computer im Netzwerk müssen die gleiche Netzmaske verwenden.

Der DEFENDO wird werkseitig mit der IP-Adresse 192.168.0.254 und der Netzmaske 255.255.255.0 ausgeliefert. Bitte beachten Sie, dass der DEFENDO es nicht unterstützt, von einem vorhanden DHCP-Server eine Adresse zu beziehen, das heißt, er kann nicht selbständig von einem bestehenden DHCP-Server automatisch beim Booten eine IP-Adresse zugeteilt bekommen. In seiner Funktion ist der DEFENDO darauf angewiesen, immer die gleiche IP-Adresse zu verwenden.

Wenn Ihr PC noch nicht über ein TCP/IP-Protokoll (siehe Netzwerkumgebung Ihres Betriebsystems) verfügt, so ist es nicht notwendig, dem PC eine passende IP-Adresse zuzuweisen. Installieren Sie in diesem Fall nur das TCP/IP-Protokoll und stellen Sie auf „IP-Adresse automatisch beziehen“. Da der DEFENDO im Auslieferungszustand als DHCP-Server fungiert, wird dem PC automatisch eine IP-Adresse zugewiesen.

6.4. Einschalten und Booten des DEFENDO

Schalten Sie hierzu auf der Rückseite des Gerätes am Netzteil den Netzschalter von der Position „0“ auf „1“. Sollte das Gerät nun nicht gleich selbständig anfangen zu booten, so betätigen Sie zusätzlich den „Power“-Schalter an der Frontseite des Gerätes.

Der Bootvorgang dauert cirka 2 Minuten. Warten Sie diese Zeit unbedingt ab, bevor Sie fortfahren!

6.5. Einstellen der IP-Adresse

Der DEFENDO hat im Auslieferungszustand die IP-Adress 192.168.0.254 mit der Netzmaske 255.255.255.0. Im allgemeinen wird es erforderlich sein, diese Einstellungen in die für Ihr LAN passenden Werte zu ändern. Es stehen dazu folgende Möglichkeiten zur Verfügung.

6.5.1. IP-Adress-Vergabe mit Hilfe des Displays

Manche DEFENDO Versionen verfügen über ein eingebautes Display. Drücken Sie den „enter“ Knopf neben dem Display um in das Menü des Displays zu gelangen. Mit Hilfe der links / rechts Knöpfe können Sie zwischen den Menüpunkten wechseln.

Wählen Sie den Menüpunkt „ip address“ und drücken Sie „enter“ um die IP Adresse zu ändern. Mit Hilfe der rauf / runter Knöpfe verändern Sie die aktuelle Ziffer der IP. Die rechts / links Knöpfe wechseln zwischen den einzelnen Ziffern. Drücken Sie „enter“ erneut, wenn die IP-Adresse fertig eingestellt ist.

Wechseln Sie nun zum Menüpunkt „netmask“ und drücken Sie „enter“ um die Netzmaske zu ändern. Mit Hilfe der rauf / runter Knöpfe verändern Sie die Netzmaske. Drücken Sie „enter“ wenn die Netmaske korrekt eingestellt ist.

Gehen Sie jetzt zum Menüpunkt “exit”, drücken Sie erneut “enter” und bestätigen Sie die Nachfrage ob die Änderungen gespeichert werden sollen. Nach einigen Sekunden ist die neue IP Adresse konfiguriert.

6.5.2. IP-Adress-Vergabe über die DEFENDO Konsole

Hierzu ist es erforderlich, Monitor und Tastatur in die entsprechenden Buchsen auf der Rückseite des DEFENDO anzuschließen. Sollte die Tastaturbuchse des DEFENDO nicht durch ein entsprechendes Piktogramm erkennbar sein, so schließen Sie die Tastatur bitte an die lila gefärbte Buchse an.

Auf dem Bildschirm sollte jetzt „login:“ erscheinen. Geben Sie als Kennung „admin“ ein. Sie werden nun nach dem zugehörigen Paßwort ge-

fragt. Im Auslieferungszustand lautet das Paßwort „redhat“. Es sollte nun eine Meldung mit der DEFENDO -Version am Bildschirm erscheinen. Geben Sie nun „ipsetup“ ein und bestätigen Sie die Eingabe. Nach kurzer Zeit werden Sie erneut um Anmeldung zur Administration gebeten. Bitte geben Sie erneut den Benutzernamen „admin“ und das zugehörige Kennwort ein. Sie sehen jetzt eine Maske mit den Grundeinstellungen des DEFENDO . Benutzen Sie die Cursor-Tasten mit dem Pfeil nach oben bzw. nach unten, um von Feld zu Feld zu navigieren. Ändern Sie die IP-Adresse und soweit erforderlich die Netzmaske auf die neuen Werte. Bewegen Sie sich dann mit den Cursortasten auf den Schalter „Apply“. Drücken Sie nun die Eingabetaste (Return) um die Änderungen zu aktivieren. Brechen Sie nun das ipsetup-Programm mit der Tastenkombination Strg-C ab und melden Sie sich durch Eingabe von „exit“ von der DEFENDO -Konsole ab. Nach ca. 30 Sekunden sollte der DEFENDO unter der neuen Adresse in Ihrem LAN erreichbar sein.

Fahren Sie bitte fort mit Kapitel 6.5.4.

6.5.3. IP-Adress-Vergabe durch umkonfigurierten PC

Sollte Ihre IP-Adresse des PCs nicht in den Bereich 192.168.0.x passen, so ist es notwendig, den Bereich des PCs kurzfristig zu ändern oder die IP-Adresse des DEFENDO mit dem auf der Install-CD mitgelieferten IP-Vergabe-Programms auf Ihr Netz einzustellen.

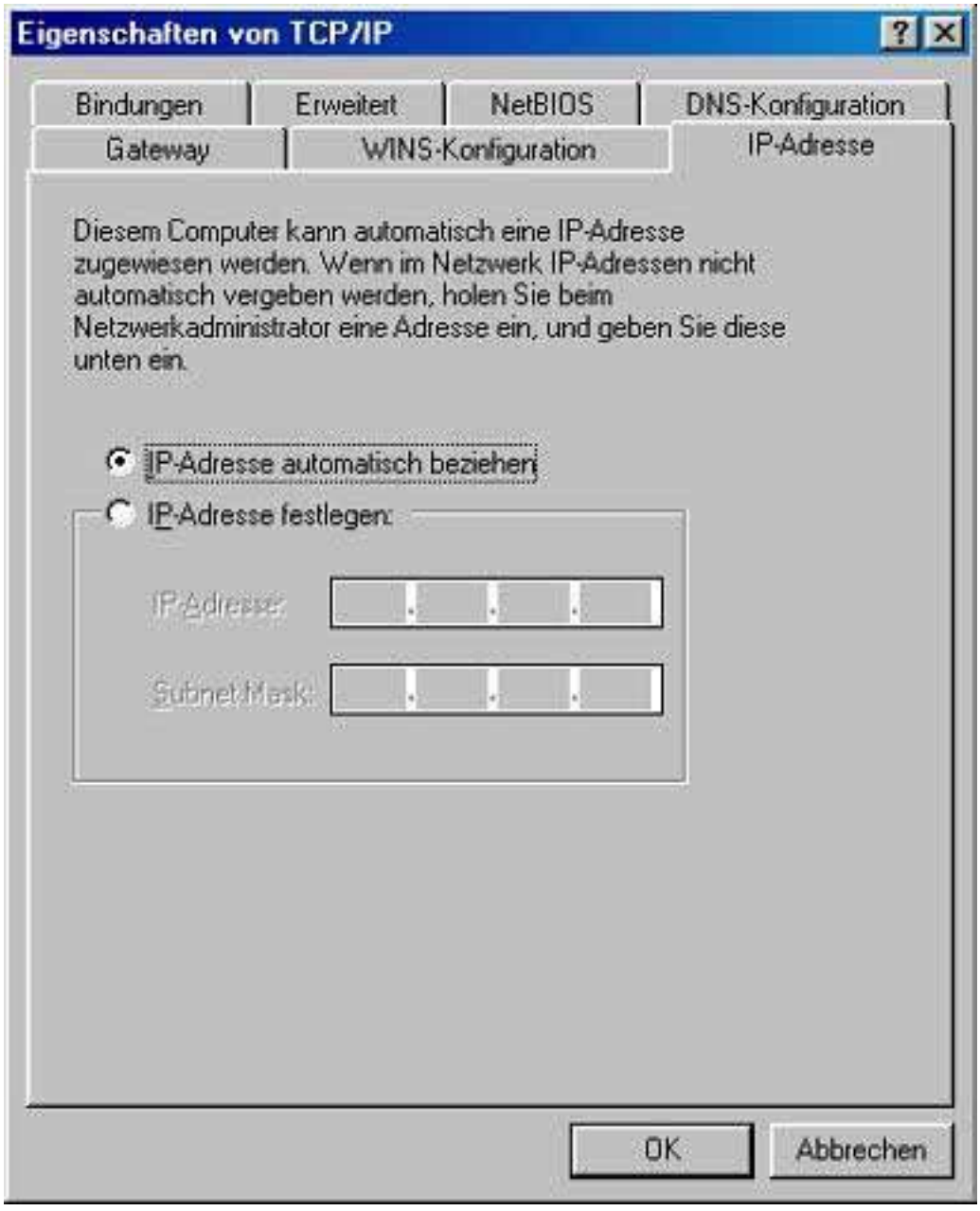
> *Hinweis:*
>
> *Bevor Sie diese Änderungen vornehmen, sollten Sie sich die IP-Adresse Ihres PCs notieren. Bitte vergewissern Sie sich, welche TCP/IP-Adresse in Ihrem Netzwerk noch zur Verfügung steht.*

Starten Sie Ihren PC und warten Sie den Boot-Vorgang ab. Gehen Sie danach über den links unten angeordneten Schalter „Start“ und „Einstellungen“ in die Systemsteuerung. Dort finden Sie das Icon „Netzwerk“. Aktivieren Sie dieses mit Hilfe des Doppelklicks. Sie erhalten folgende Maske:

Selektieren Sie den Eintrag „TCP/IP“ in Verbindung mit Ihrer Netzwerkkarte aus und wählen Sie den Schalter „Eigenschaften“.

Aktivieren Sie nach dem Aufruf des Icons „Netzwerk“ in der Systemsteuerung den Reiter „Protokolle“. Wählen Sie hierzu den Eintrag „TCP/IP-Protokoll.

Nach Anwahl des Schalters „Eigenschaften“ erhalten Sie folgende Maske:



Sollte wie hier in diesem Beispiel der Punkt „IP-Adresse automatisch beziehen“ selektiert sein, so ist es nicht notwendig, die eingestellte IP-Adresse zu notieren, da sie automatisch zugewiesen wird.

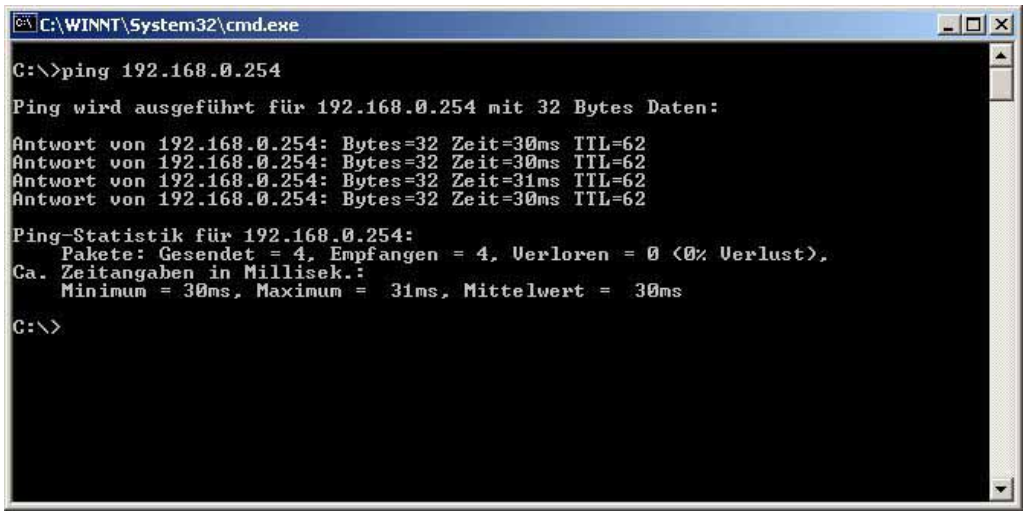
Wählen Sie das Optionsfeld „IP-Adresse festlegen“ und tragen Sie im Feld IP-Adresse z. B. die „192.168.0.1“ (auf keinen Fall die 192.168.0.254, da diese durch den DEFENDO belegt ist) sowie unter Subnet-Mask den Wert „255.255.255.0“ ein. Wenn eine feste Adresse in dieser Maske eingetragen ist, so notieren Sie sich diese bitte (mit der dazugehörigen Subnet-Mask) und folgen den Schritten wie gerade beschrieben.

Wählen Sie unter dem Listenfeld „Adapter“ die entsprechende Netzwerkkarte aus und führen Sie die Einstellungen wenn notwendig wie oben beschrieben aus.

6.5.4. Überprüfung der Verbindung zum DEFENDO

Die Überprüfung der Verbindung des PCs an den DEFENDO kann mit Hilfe des „Ping“-Befehls ausgeführt werden. Starten Sie hierzu ein MS-DOS-Eingabefenster. Wählen Sie den Schalter „Start“ und den Menüpunkt „Ausführen“. Unter Windows 9x tragen Sie den Befehl „Command“ ein. Unter Windows NT 4.0 empfiehlt sich der Aufruf „Cmd“. Bestätigen Sie Ihre Eingabe mit dem Schalter „OK“.

Sie erhalten nun ein DOS-Emulationsfenster. Führen Sie hier folgenden Befehl aus: „PING 192.168.0.254“ und bestätigen Sie ihn mit der Eingabetaste. Haben Sie die IP-Adresse des DEFENDO bereits geändert so verwenden Sie bitte die geänderte Adresse anstelle der 192.168.0.254. Sollten alle Einstellungen korrekt sein, so erhalten Sie folgende Bildschirmmeldungen („Antwort von...“):

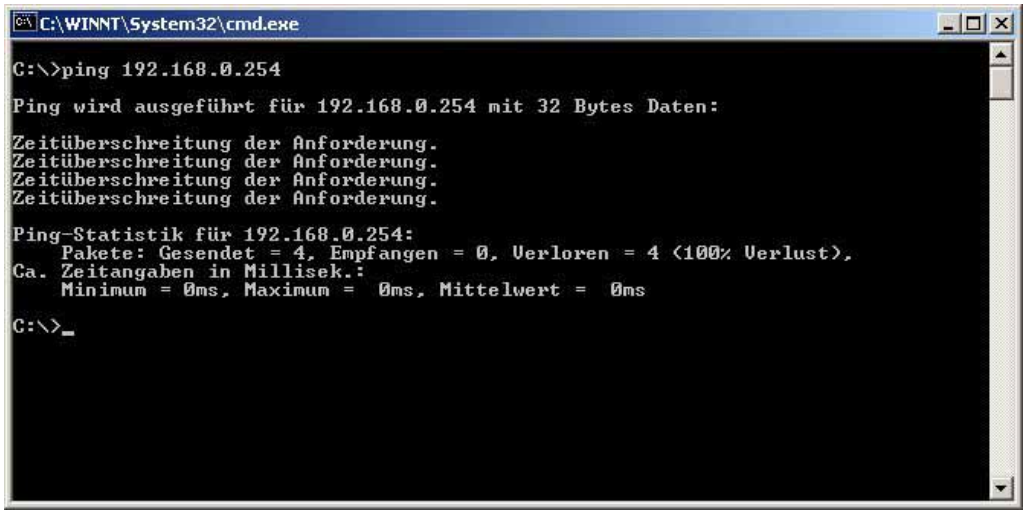

C:\WINNT\System32\cmd.exe
C:\>ping 192.168.0.254
Ping wird ausgeführt für 192.168.0.254 mit 32 Bytes Daten:
Antwort von 192.168.0.254: Bytes=32 Zeit=30ms TTL=62
Antwort von 192.168.0.254: Bytes=32 Zeit=30ms TTL=62
Antwort von 192.168.0.254: Bytes=32 Zeit=31ms TTL=62
Antwort von 192.168.0.254: Bytes=32 Zeit=30ms TTL=62
Ping-Statistik für 192.168.0.254:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 30ms, Maximum = 31ms, Mittelwert = 30ms
C:\>

Hinweis:

Ping-Befehl unter Windows NT 4.0

Hierbei sind englische Meldungen normal.

Sollte eine falsche IP-Adresse angegeben worden sein, oder die Verbindung nicht zustande kommen, erhalten Sie folgende Meldungen („Zeitüberschreitung der Anforderung“):


C:\WINNT\System32\cmd.exe
C:\>ping 192.168.0.254
Ping wird ausgeführt für 192.168.0.254 mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Ping-Statistik für 192.168.0.254:
Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4 (100% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
C:\>

Hinweis:

Ping-Befehl unter Windows NT 4.0 Hierbei sind englische Meldungen normal (no reply)

In diesem Fall überprüfen Sie bitte die oben genannten Einstellungen bzw. wiederholen Sie diese. Überprüfen Sie auch den Anschluss des DEFENDO am Hub bzw. am Switch, ob die Link-LED leuchtet sowie die Link-LED an der Netzwerkkarte des DEFENDO. Sollte bereits eine Firewall in Ihrem System installiert sein, so überprüfen Sie bitte, dass diese das „Pingen“ auch zulässt.

6.5.5. Starten der WEB-Oberfläche des DEFENDO

Nun kann die Konfigurationen des DEFENDO mit Hilfe Ihres Internet-Browsers eingerichtet werden. Starten Sie hierzu Ihren Internetbrowser.

Hinweis:

Sollte Ihr PC noch nicht auf den Internetzugang konfiguriert worden sein, meldet sich der „Internet-Assistent“. Er will Sie durch die Konfiguration führen. Folgen Sie ihm und wählen an der entsprechenden Abfrage den Eintrag „über LAN verbinden“. Nehmen Sie jedoch noch keine Einträge vor! Vergewissern Sie sich, dass Sie die richtige Version des Browsers installiert haben!

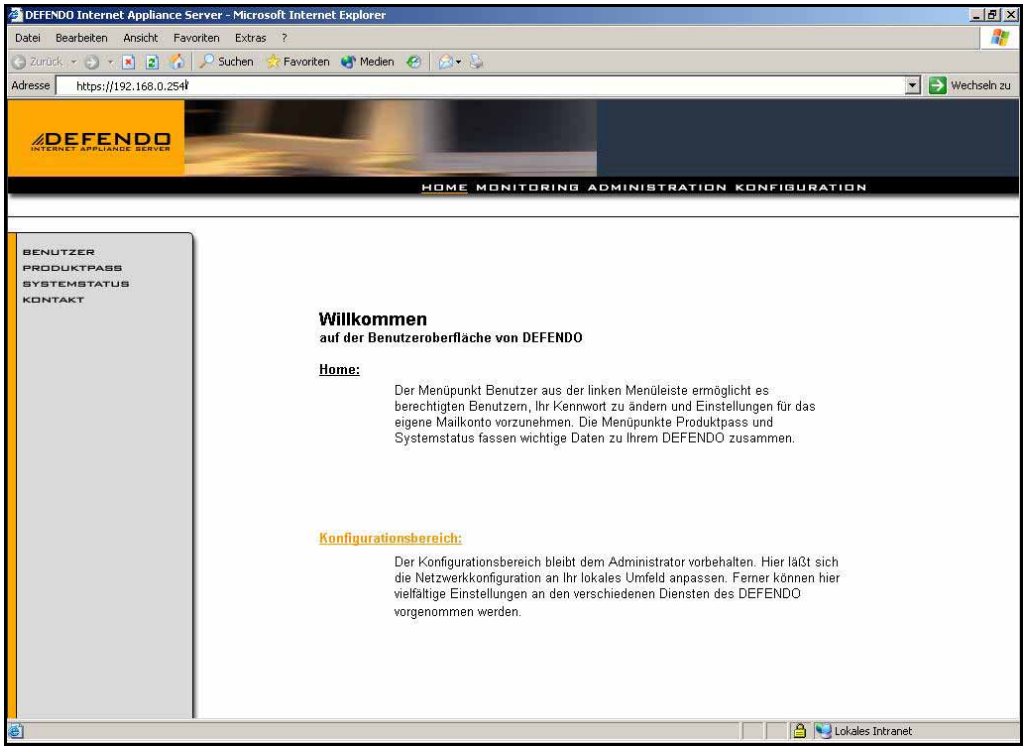
Tragen Sie im Feld Location bzw. Adresse die folgende Zeile ein (sofern Sie die IP-Adresse des DEFENDO bereits verändert haben so verwenden Sie bitte die neue Adressen anstelle von 192.168.0.254):

https://192.168.0.254

Hinweis:

Der Zugriff auf die Administrationsoberfläche erfolgt verschlüsselt mit „https://“. Diese Angabe ist unbedingt notwendig! Ein Zugriff auf die Administrationsoberfläche mit „http://“ (ohne s) ist auf diese Weise nicht möglich.

Sie erhalten nun die Startseite des DEFENDO .


DEFENDO Internet Appliance Server - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Suchen Favoriten Medien
Adresse https://192.168.0.254
Wechseln zu
DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
BENUTZER
PRODUKTPASS
SYSTEMSTATUS
KONTAKT
Willkommen
auf der Benutzeroberfläche von DEFENDO
Home:
Der Menüpunkt Benutzer aus der linken Menüleiste ermöglicht es berechtigten Benutzern, Ihr Kennwort zu ändern und Einstellungen für das eigene Mailkonto vorzunehmen. Die Menüpunkte Produktpass und Systemstatus fassen wichtige Daten zu Ihrem DEFENDO zusammen.
Konfigurationsbereich:
Der Konfigurationsbereich bleibt dem Administrator vorbehalten. Hier läßt sich die Netzwerkkonfiguration an Ihr lokales Umfeld anpassen. Ferner können hier vielfältige Einstellungen an den verschiedenen Diensten des DEFENDO vorgenommen werden.
Lokales Intranet

Hinweis:

Die Oberfläche ist nicht für die gleichzeitige Bedienung von mehreren Browsern aus konzipiert. Eine gleichzeitige Konfiguration ist zwar in den meisten Bereichen unproblematisch, insbesondere die parallele Konfiguration im gleichen Bereichen kann jedoch problematisch sein.

Auch die Verwendung der „Zurück"-Schaltfläche des Browsers nach dem Bestätigen von Änderungen kann zu Problemen führen.

6.5.6. Erste Einstellungen des DEFENDO

Um die wichtigsten Grundfunktionen des DEFENDO einzustellen, verwenden Sie bitte den Menüpunkt „Konfiguration". Gehen Sie die nun folgenden Konfigurations-Assistenten der Reihe nach durch. Somit ist sichergestellt, dass Netzwerkanbindung, Fernwartung und Internetzugang sowie E-Mail ohne Falscheingaben konfiguriert werden können.

Danach ist der DEFENDO in der Grundkonfiguration betriebsbereit.

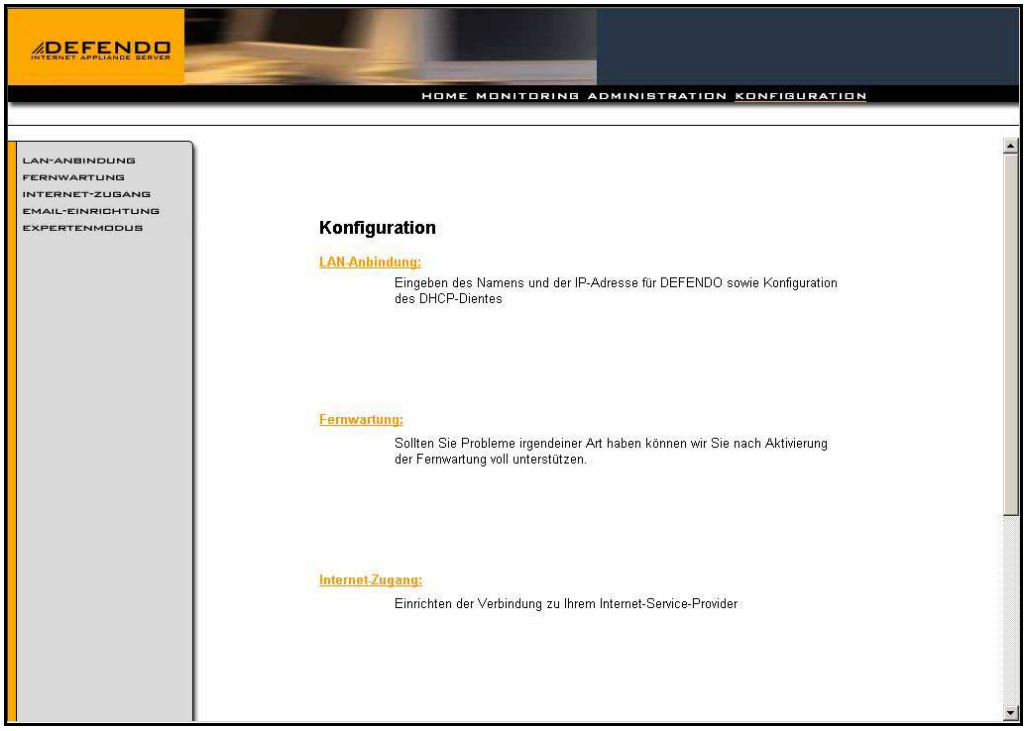
7. Das Hauptmenü „Konfiguration“

Der DEFENDO hat für die wichtigsten Funktionen Konfigurations-Assistenten, die es auch Administratoren mit weniger Netzwerkerfahrung ermöglichen sollen den DEFENDO einzurichten. Bitte lesen Sie die Seiten des Konfigurations-Assistenten vollständig durch, Sie enthalten sehr viele nützliche Informationen.

7.1. Der Konfigurations-Assistent „LAN-Anbindung“

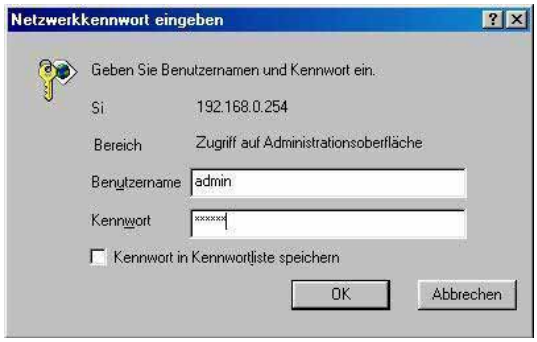
Dieser Konfigurations-Assistent unterstützt Sie bei der Anbindung des DEFENDO an Ihr Netzwerk. Sie vergeben die IP-Adresse mit der Ihr DEFENDO in Ihrem LAN erreichbar sein soll und weisen ihm einen Namen und eine Internet-Domäne zu. Ferner teilen Sie dem DEFENDO mit, welchen IP-Adressbereich die Intranet-Dienste zur Verfügung haben sollen. Schließlich können Sie den DHCP-Dienst konfigurieren oder deaktivieren. Dieser ist zuständig für die automatische IP-Adressvergabe an die Workstations (PCs) in Ihrem LAN.

Bewegen Sie sich mit Hilfe der Maus zur Menüleiste auf dem Eintrag „Konfiguration“ und bestätigen Sie dort mit einem Mausklick. Der DEFENDO wechselt nun in die Konfigurations-Untermaske.



Bestätigen Sie den Schalter „LAN-Anbindung“. Da es Ihre erste administrative Einstellung am DEFENDO ist, will er von Ihnen einen Benutzer sowie ein Passwort wissen, dessen Konto berechtigt ist, Systemeinstellungen vorzunehmen. Wie bereits im Kapitel 4.5 beschrieben, lautet der Benutzer „admin“ und das Standardpasswort „redhat“.

Aktivieren Sie den Haken bei „Kennwort in der Kennwortliste speichern“ in der nachfolgenden Maske ***nicht***, da sonst von Ihrem PC aus die Administration des DEFENDO immer ohne Sicherheitsabfrage erfolgen könnte. Für die Administration des DEFENDO ist eine Anmeldung an Ihrem Netzwerk nicht notwendig! Tragen Sie Benutzer und Passwort in die entsprechenden Felder ein:

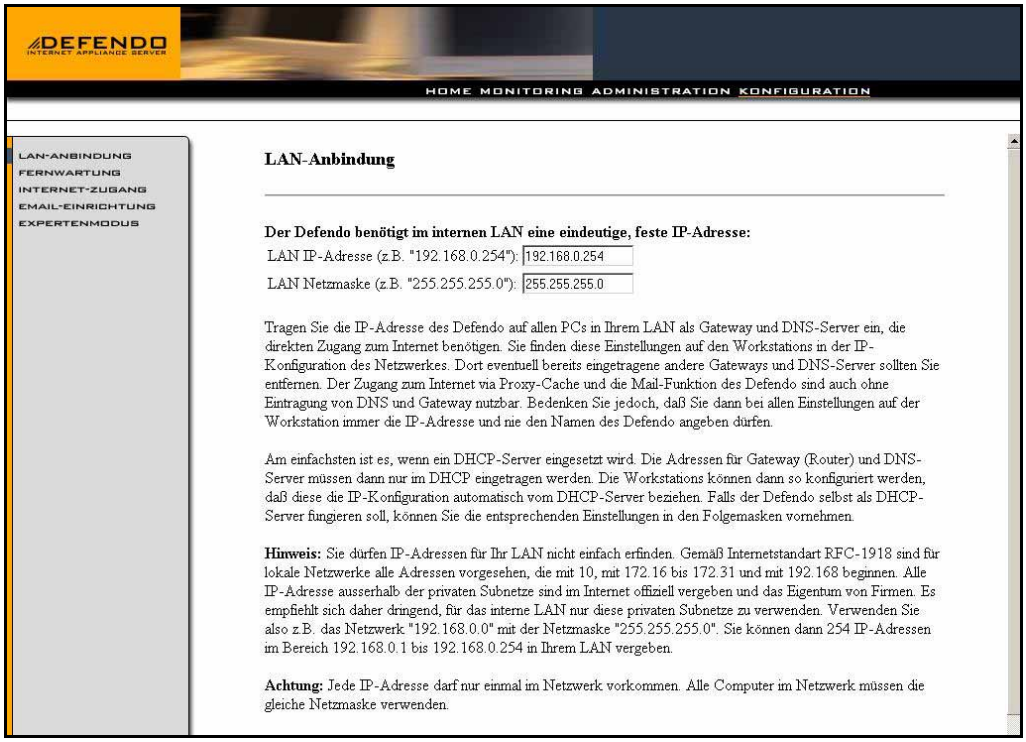


Nach erfolgter Anmeldung wird der Konfigurations-Assistent zur LAN-Anbindung gestartet.

7.1.1. Vergabe der IP-Adresse des DEFENDO

In der nun erscheinenden Seite muss die neue IP-Adresse des DEFENDO sowie die Subnet-Mask eingetragen werden.

> *Hinweis:*
>
> *Der DEFENDO benötigt im internen LAN eine eindeutige, feste IP-Adresse! Vergeben Sie keine Adresse, die sich bereits in Ihrem LAN (Local Area Network) befindet. Fragen Sie bei Zweifeln Ihren Netzwerkadministrator.*


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
LAN-Anbindung
Der Defendo benötigt im internen LAN eine eindeutige, feste IP-Adresse:
LAN IP-Adresse (z.B. "192.168.0.254"): 192.168.0.254
LAN Netzmaske (z.B. "255.255.255.0"): 255.255.255.0
Tragen Sie die IP-Adresse des Defendo auf allen PCs in Ihrem LAN als Gateway und DNS-Server ein, die direkten Zugang zum Internet benötigen. Sie finden diese Einstellungen auf den Workstations in der IP-Konfiguration des Netzwerkes. Dort eventuell bereits eingetragene andere Gateways und DNS-Server sollten Sie entfernen. Der Zugang zum Internet via Proxy-Cache und die Mail-Funktion des Defendo sind auch ohne Eintragung von DNS und Gateway nutzbar. Bedenken Sie jedoch, daß Sie dann bei allen Einstellungen auf der Workstation immer die IP-Adresse und nie den Namen des Defendo angeben dürfen.
Am einfachsten ist es, wenn ein DHCP-Server eingesetzt wird. Die Adressen für Gateway (Router) und DNS-Server müssen dann nur im DHCP eingetragen werden. Die Workstations können dann so konfiguriert werden, daß diese die IP-Konfiguration automatisch vom DHCP-Server beziehen. Falls der Defendo selbst als DHCP-Server fungieren soll, können Sie die entsprechenden Einstellungen in den Folgemasken vornehmen.
Hinweis: Sie dürfen IP-Adressen für Ihr LAN nicht einfach erfinden. Gemäß Internetstandart RFC-1918 sind für lokale Netzwerke alle Adressen vorgesehen, die mit 10, mit 172.16 bis 172.31 und mit 192.168 beginnen. Alle IP-Adresse ausserhalb der privaten Subnetze sind im Internet offiziell vergeben und das Eigentum von Firmen. Es empfiehlt sich daher dringend, für das interne LAN nur diese privaten Subnetze zu verwenden. Verwenden Sie also z.B. das Netzwerk "192.168.0.0" mit der Netzmaske "255.255.255.0". Sie können dann 254 IP-Adressen im Bereich 192.168.0.1 bis 192.168.0.254 in Ihrem LAN vergeben.
Achtung: Jede IP-Adresse darf nur einmal im Netzwerk vorkommen. Alle Computer im Netzwerk müssen die gleiche Netzmaske verwenden.

Tragen Sie die von Ihnen gewünschte IP-Adresse des DEFENDO in das entsprechende Feld sowie in das darauf folgende Feld der Subnet-Mask-Adresse passend zu Ihren Netzwerk ein.

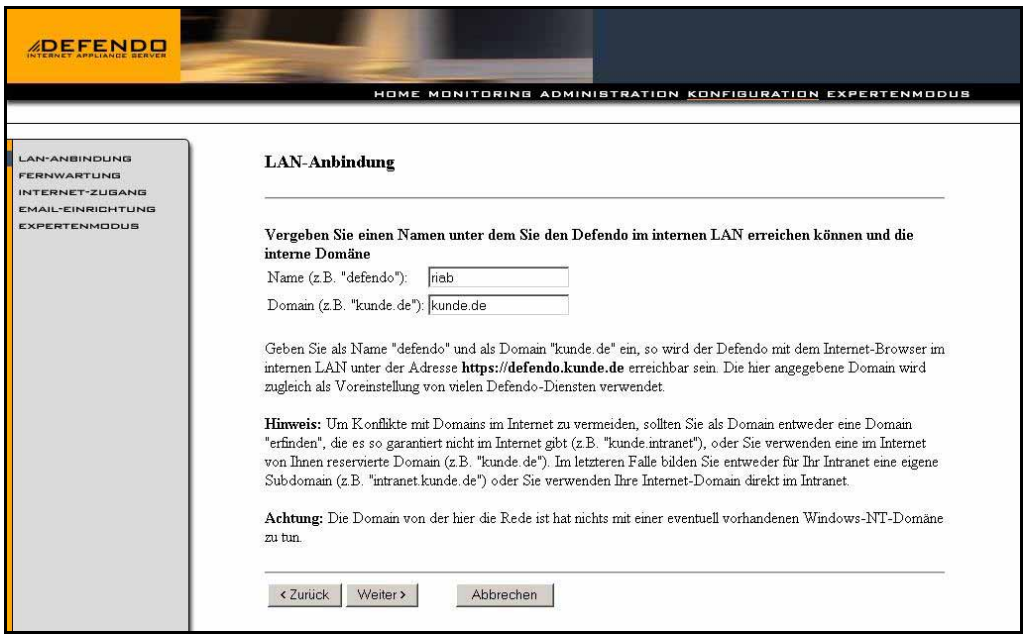
Bestätigen Sie Ihre Eingabe mit dem Schalter „Weiter“, den Sie am Ende dieser Seite finden.

7.1.2. Vergabe des Domänen-Namens Ihres LANs

Geben Sie als Name z. B. „DEFENDO „ und als Domain z. B. „muster.de“ ein, so wird der DEFENDO mit dem Internet-Browser im internen LAN unter der Adresse „https://DEFENDO.muster.de**“** erreichbar sein. Sollten Sie bereits eine Domain bei einem Provider reserviert bzw. konnektiert haben, verwenden Sie bitte diese.

Hinweis:

Um Konflikte mit Domains im Internet zu vermeiden, sollten Sie als Domain entweder eine Domain „erfinden“, die es so garantiert (siehe WWW.DENIC.DE“) nicht im Internet gibt, oder Sie verwenden eine im Internet von Ihnen reservierte Domain (z. B.“muster.de“). Bitte beachten Sie, dass über WWW.DENIC.DE nur deutsche Domains (.DE) abgefragt werden können.*


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION EXPERTENMODUS
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
LAN-Anbindung
Vergeben Sie einen Namen unter dem Sie den Defendo im internen LAN erreichen können und die interne Domäne
Name (z.B. "defendo"): riab
Domain (z.B. "kunde.de"): kunde.de
Geben Sie als Name "defendo" und als Domain "kunde.de" ein, so wird der Defendo mit dem Internet-Browser im internen LAN unter der Adresse https://defendo.kunde.de erreichbar sein. Die hier angegebene Domain wird zugleich als Voreinstellung von vielen Defendo-Diensten verwendet.
Hinweis: Um Konflikte mit Domains im Internet zu vermeiden, sollten Sie als Domain entweder eine Domain "erfinden", die es so garantiert nicht im Internet gibt (z.B. "kunde.intranet"), oder Sie verwenden eine im Internet von Ihnen reservierte Domain (z.B. "kunde.de"). Im letzteren Falle bilden Sie entweder für Ihr Intranet eine eigene Subdomain (z.B. "intranet.kunde.de") oder Sie verwenden Ihre Internet-Domain direkt im Intranet.
Achtung: Die Domain von der hier die Rede ist hat nichts mit einer eventuell vorhandenen Windows-NT-Domäne zu tun.
< Zurück
Weiter >
Abbrechen

Im letzteren Falle bilden Sie entweder für Ihr Intranet eine eigene Subdomain (z.B. „intranet.muster.de“) oder Sie verwenden Ihre Internet-Domain direkt im Intranet.

Hinweis:

Die Domain von der hier die Rede ist hat nichts mit einer eventuell vorhandenen Windows-NT 4.0-Domäne zu tun.

Bestätigen Sie Ihre Eingaben mit dem Schalter „Weiter“ am Ende dieser Seite.

7.1.3. IP-Adressen des internen LANs definieren

Damit der DEFENDO unterscheiden kann, ob ein Zugriff aus dem Internet oder dem internen LAN erfolgt, werden hier die Netzwerke eingetragen, die dem LAN zuzurechnen sind. Manche Dienste, wie z.B. der Web-Server des DEFENDO , bieten spezielle Bereiche nur den hier angegebenen lokalen Netzwerken an. Andere Dienste wie der Proxy-Cache und die Windows-Freigaben verweigern IP-Adressen außerhalb der hier angegebenen Adressbereiche völlig ihre Dienste.

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
LAN-Anbindung
Geben Sie bitte die IP-Subnetze ein, die der Defendo als Intranet betrachten soll
Netzwerk-Adressen / Netzmasken der lokalen Netze (z.B. "192.168.0.0/255.255.255.0"):
/
Hinzufügen
192.168.0.0/255.255.0.0
172.16.0.0/255.240.0.0
10.0.0.0/255.0.0.0
Entfernen
Damit der Defendo unterscheiden kann, ob ein Zugriff aus dem Internet oder dem internen LAN erfolgt, werden hier die Netzwerke eingetragen, die dem LAN zuzurechnen sind. Manche Dienste, wie z.B. der Web-Server des Defendo, bieten spezielle Bereiche nur den hier angegebenen lokalen Netzwerken an. Andere Dienste wie der Proxy-Cache und die Windows-Freigaben verweigern bei IP-Adressen außerhalb der hier angegebenen Adressbereiche völlig ihre Dienste.
Achtung: Sollten Sie versehentlich das Netzwerk entfernen in dem Sie sich selbst befinden und Sie erhalten beim Zugriff auf die Administrationsoberfläche eine Fehlermeldung vom Proxy-Cache, dann deaktivieren Sie bitte vorübergehend die Verwendung des Proxy-Caches in Ihrem Web-Browser.
< Zurück
Weiter >
Abbrechen

Tragen Sie hier die Adresse Ihres LANs ein. Im unteren Feld ist die Subnet-Maske einzutragen. Sollten hier Standard-Einträge vorhanden sein, die für Ihr LAN nicht zutreffen oder gewollt sind, so selektieren Sie diese und verwenden Sie den Schalter „Entfernen“ zum Löschen die-

ser. Verwenden Sie zum Hinzufügen Ihrer Einstellungen den Schalter „Hinzufügen“. Der DEFENDO wechselt in die nächste Konfigurationsmaske mit dem Schalter „Weiter“.

> *Hinweis:*
>
> *Sollten Sie versehentlich das Netzwerk entfernen in dem Sie sich selbst befinden und eine Fehlermeldung beim Zugriff auf die Administrationsoberfläche vom Proxy-Cache erhalten, dann deaktivieren Sie bitte vorübergehend die Verwendung des Proxy-Caches in Ihrem Web-Browser.*

7.1.4. Der DHCP-Dienst des DEFENDO

Mit Hilfe des DHCP-Dienstes des DEFENDO läßt sich die IP-Konfiguration (bzw. die IP-Adress-Vergabe) der Workstations (PCs) im LAN zentral verwalten und automatisieren. Der DEFENDO kann diese Aufgabe in Ihrem LAN übernehmen, wenn dies noch nicht von einem anderen Server übernommen wird.

Sollte sich in Ihrem LAN bereits ein DHCP-Server befinden, kann der DHCP-Server des DEFENDO auch als „Secondary DHCP-Server“ konfiguriert werden. Auf diese Weise kann im Falle eines Ausfalles des primären DHCP-Servers immer noch der DHCP-Dienst aufrecht erhalten werden.

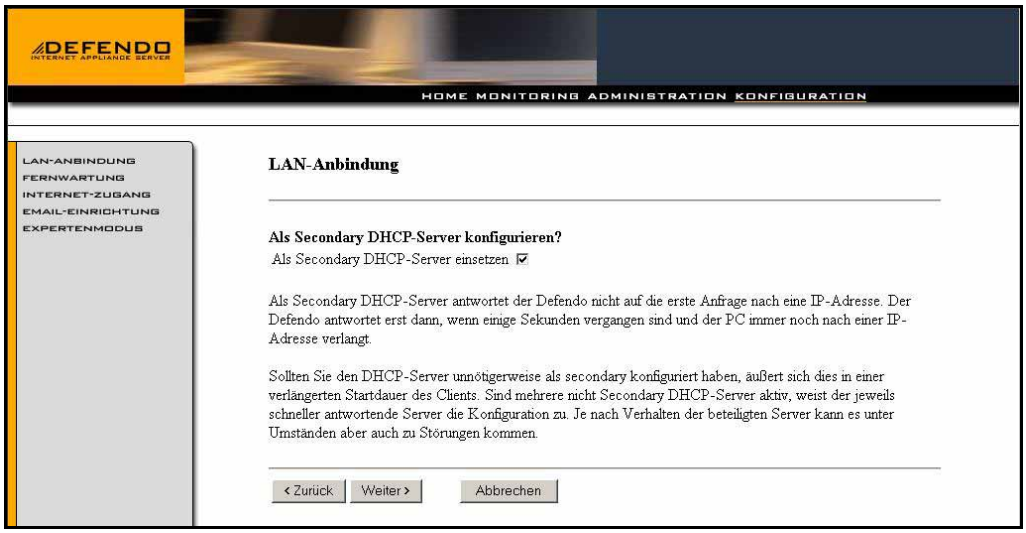
Sollten Sie den DHCP-Dienst des DEFENDO nicht in Anspruch nehmen wollen, so wählen Sie in der angezeigten Maske den Eintrag „Nein“. Bestätigen Sie Ihre Auswahl mit dem Schalter „Weiter“ am Ende dieser Seite. Lesen Sie in diesem Falle weiter im Kapitel 7.1.5.

DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
LAN-Anbindung
Wollen Sie den DHCP-Dienst des Defendo verwenden?
DHCP aktivieren Ja
Nein
Mit Hilfe des DHCP-Dienstes läßt sich die IP-Konfiguration von Computern im LAN zentral verwalten. Der Defendo kann diese Aufgabe in Ihrem LAN übernehmen wenn dies noch nicht von einem anderen Server angeboten wird. Sollte sich in Ihrem LAN bereits ein DHCP-Server befinden, kann der DHCP-Server des Defendo auch als secondary DHCP-Server konfiguriert werden. In diesem Falle verteilt der Defendo die IP-Adressen nur, wenn der eigentliche DHCP-Server ausgefallen ist.
< Zurück
Weiter >
Abbrechen

Falls Sie den DHCP-Dienst des DEFENDO doch in Anspruch nehmen wollen, so wählen Sie den Eintrag „Ja“ und bestätigen Sie Ihre Auswahl mit den Schalter „Weiter“ am Ende dieser Seite.

7.1.4.1. Verwenden des sekundären DHCP-Dienstes

Setzen Sie in der nun angezeigten Maske den Haken im Eintrag „Als Secondary DHCP-Server einsetzen“ und wählen Sie den Schalter „Weiter“.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
LAN-Anbindung
Als Secondary DHCP-Server konfigurieren?
Als Secondary DHCP-Server einsetzen
Als Secondary DHCP-Server antwortet der Defendo nicht auf die erste Anfrage nach eine IP-Adresse. Der Defendo antwortet erst dann, wenn einige Sekunden vergangen sind und der PC immer noch nach einer IP-Adresse verlangt.
Sollten Sie den DHCP-Server unnötigerweise als secondary konfiguriert haben, äußert sich dies in einer verlängerten Startdauer des Clients. Sind mehrere nicht Secondary DHCP-Server aktiv, weist der jeweils schneller antwortende Server die Konfiguration zu. Je nach Verhalten der beteiligten Server kann es unter Umständen aber auch zu Störungen kommen.
< Zurück
Weiter >
Abbrechen

Es besteht nur ein Unterschied zum primären DHCP-Dienst. Als „Secondary DHCP-Server“ antwortet der DEFENDO nicht auf die erste Anfrage eines Gerätes nach eine IP-Adresse. Der DEFENDO antwortet erst dann, wenn einige Sekunden vergangen sind und das Gerät immer noch nach einer IP-Adresse verlangt. In diesem Falle geht der DEFENDO davon aus, dass der eigentliche DHCP-Server nicht verfügbar ist und weist eine IP-Adresse zu. Bitte beachten Sie, dass sich die dynamisch zugewiesenen IP-Adressbereiche des primären und des sekundären DHCP-Servers nicht überschneiden dürfen, da der primäre Server ja nichts von der Existenz des sekundären weiß. Folglich kann es bei Überschneidungen zu Konflikten kommen.

Hinweis:

Sollten Sie den DHCP-Server unnötigerweise als „Secondary DHCP-Server“ konfiguriert haben, äußert sich dies in einer verlängerten Startdauer der Clients. Sind mehrere nicht „Secondary DHCP-Server“ aktiv, weist der jeweils schneller antwortende Server die Konfiguration bzw. IP-Adressierung zu. Je nach Verhalten der beteiligten Server kann es unter Umständen aber auch zu Störungen kommen.

Zur weiteren Konfiguration lesen Sie bitte das nachfolgende Kapitel.

7.1.4.2. Verwenden des primären DHCP-Dienstes

Entfernen Sie in der nun angezeigten Maske den Haken im Eintrag „Als Secondary DHCP-Server einsetzen“ und wählen Sie den Schalter „Weiter“.

Sie sollten Servern, sowie Netzwerkdruckern, Hubs und Switches feste Adressen zuteilen, da diese Geräte in der Regel nicht variieren oder ausgetauscht werden und dann immer unter der gleichen IP-Adresse erreichbar sind. Der Einsatz des DHCP-Dienstes empfiehlt sich hauptsächlich für die Workstations (PCs) des Netzwerkes. Hier kommt es eher vor, dass Geräte ausgetauscht werden (Erneuerung, Defekt des Gerätes, etc.).

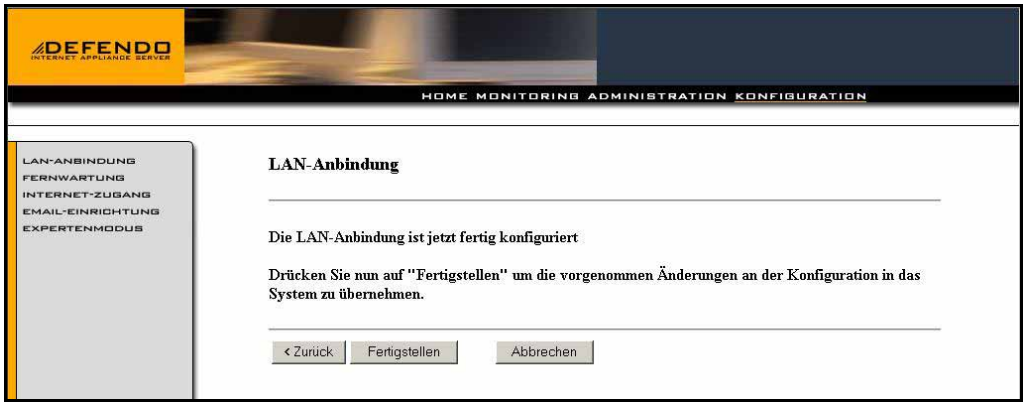
Hinweis:

Dimensionieren Sie den Bereich für die Anzahl der Geräte in Ihrem Netzwerk entsprechend groß! Ein zu klein gewählter Bereich führt dazu, dass nicht alle Geräte mit einer IP-Adresse versorgt werden können und somit nicht mit dem IP-Protokoll Verbindung zum Internet oder zu Servern haben!

Tragen Sie in der Maske die Anfangsadresse (z. B. 192.168.0.100) des Bereiches sowie die Endadresse (z. B. 192.168.0.199) ein. Bestätigen Sie Ihre Angaben mit dem Schalter „Hinzufügen“. Somit würden Ihnen 100 Adressen zur Verfügung stehen. Natürlich können Sie auch mehrere Bereiche angeben, um so z. B. Ausschlussadressen bereitzustellen.

7.1.5. LAN-Anbindung fertigstellen

Nach Anwahl des Schalters „Weiter“ sind die LAN-Einstellungen konfiguriert und können gespeichert werden. Bestätigen Sie dies über den Schalter „Fertigstellen“.



Hinweis:

Sollte die IP-Adresse des DEFENDO durch Sie geändert worden sein, ist der DEFENDO nun nicht mehr ansprechbar. Es muss in diesem Falle auch die IP-Adresse des Konfigurations-PCs wieder umkonfiguriert werden. Zur Vorgehensweise lesen Sie bitte im Kapitel 6.5 nach.

Wenn keine Änderung der IP-Adresse des DEFENDO vorgenommen wurde, so kann gleich mit der weiteren Konfiguration des DEFENDO fortgefahren werden. Ansonsten muss der PC neu gestartet werden. Danach müssen Sie die Web-Oberfläche des DEFENDO mit Hilfe Ihres Browers neu aufbauen.

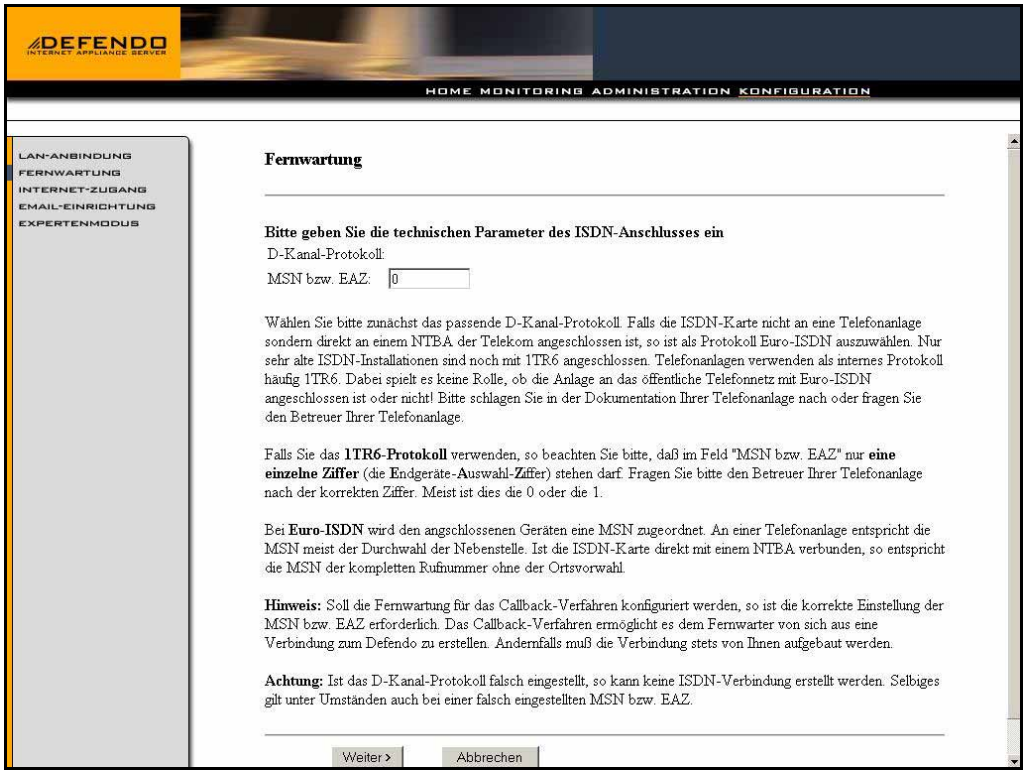
7.2. Der Konfigurations-Assistent „Fernwartung“

Mit Hilfe dieses Konfigurations-Assistenten können Sie den Fernwartungszugang für Ihren Support (siehe Kapitel 14) einrichten. Er ist nützlich, wenn Sie Probleme mit der Konfiguration des DEFENDO haben.

Wählen Sie hierzu in der Konfigurations-Assistenten-Maske den Eintrag „Fernwartung“.

Bestätigen Sie Ihre Anwahl mit den Schalter „Weiter“ und Sie gelangen in die eigentlichen Konfigurationsmasken. Hierzu benötigen Sie folgende Angaben:

- Die MSN oder EAZ Ihres ISDN-Anschlusses
- Das verwendete D-Kanal-Protokoll (ISDN)
- Gegebenenfalls Ihre Support-Rufnummer


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Fernwartung
Bitte geben Sie die technischen Parameter des ISDN-Anschlusses ein
D-Kanal-Protokoll:
MSN bzw. EAZ: 0
Wählen Sie bitte zunächst das passende D-Kanal-Protokoll. Falls die ISDN-Karte nicht an eine Telefonanlage sondern direkt an einem NTBA der Telekom angeschlossen ist, so ist als Protokoll Euro-ISDN auszuwählen. Nur sehr alte ISDN-Installationen sind noch mit 1TR6 angeschlossen. Telefonanlagen verwenden als internes Protokoll häufig 1TR6. Dabei spielt es keine Rolle, ob die Anlage an das öffentliche Telefonnetz mit Euro-ISDN angeschlossen ist oder nicht! Bitte schlagen Sie in der Dokumentation Ihrer Telefonanlage nach oder fragen Sie den Betreuer Ihrer Telefonanlage.
Falls Sie das 1TR6-Protokoll verwenden, so beachten Sie bitte, daß im Feld "MSN bzw. EAZ" nur eine einzelne Ziffer (die Endgeräte-Auswahl-Ziffer) stehen darf. Fragen Sie bitte den Betreuer Ihrer Telefonanlage nach der korrekten Ziffer. Meist ist dies die 0 oder die 1.
Bei Euro-ISDN wird den angschlossenen Geräten eine MSN zugeordnet. An einer Telefonanlage entspricht die MSN meist der Durchwahl der Nebenstelle. Ist die ISDN-Karte direkt mit einem NTBA verbunden, so entspricht die MSN der kompletten Rufnummer ohne der Ortsvorwahl.
Hinweis: Soll die Fernwartung für das Callback-Verfahren konfiguriert werden, so ist die korrekte Einstellung der MSN bzw. EAZ erforderlich. Das Callback-Verfahren ermöglicht es dem Fernwarter von sich aus eine Verbindung zum Defendo zu erstellen. Andernfalls muß die Verbindung stets von Ihnen aufgebaut werden.
Achtung: Ist das D-Kanal-Protokoll falsch eingestellt, so kann keine ISDN-Verbindung erstellt werden. Selbiges gilt unter Umständen auch bei einer falsch eingestellten MSN bzw. EAZ.
Weiter >
Abbrechen

7.2.1. Einrichten des Protokolls und der MSN/EAZ

Wählen Sie bitte zunächst das passende D-Kanal-Protokoll. Falls die ISDN-Karte des DEFENDO nicht an eine Telefonanlage sondern direkt an einem NTBA der Telekom angeschlossen ist, so ist als Protokoll Euro-ISDN auszuwählen. Nur sehr alte ISDN-Installationen sind noch mit 1TR6 angeschlossen. Telefonanlagen verwenden als internes Protokoll häufig 1TR6. Dabei spielt es keine Rolle, ob die Anlage an das öffentliche Telefonnetz mit Euro-ISDN angeschlossen ist oder nicht! In Amerika ist das Protokoll NI1 zu verwenden. Bitte schlagen Sie in der Dokumentation Ihrer Telefonanlage nach oder fragen Sie den Betreuer Ihrer Telefonanlage.

Falls Sie das 1TR6-Protokoll verwenden, so beachten Sie bitte, dass in der Regel im Feld „MSN bzw. EAZ“ nur eine einzelne Ziffer (die Endgeräte-Auswahl-Ziffer) stehen darf. Fragen Sie bitte den Betreuer Ihrer Telefonanlage nach der korrekten Ziffer. Meist ist dies die 0 oder die 1. Bei Euro-ISDN wird den angeschlossenen Geräten eine MSN zugeordnet. An einer Telefonanlage entspricht die MSN meist der Durchwahl der Nebenstelle. Ist die ISDN-Karte direkt mit einem NTBA verbunden, so entspricht die MSN der kompletten Rufnummer ohne der Ortsnetzvorwahl. Für das amerikanische NI1 Protokoll ist die Angabe der MSN sowie des SPID (Service Point Identifier) im Format MSN:SPID erforderlich.

Hinweis:

Soll die Fernwartung für das Callback-Verfahren konfiguriert werden, so ist die korrekte Einstellung der MSN bzw. EAZ zwingend erforderlich. Das Callback-Verfahren (Rückrufverfahren) ermöglicht es dem Fernwarter von sich aus eine Verbindung zum DEFENDO zu erstellen. Wollen Sie das nicht, so muss die Verbindung stets von Ihnen aufgebaut werden!

Ist das D-Kanal-Protokoll falsch eingestellt, so kann keine ISDN-Verbindung erstellt werden. Selbiges gilt unter Umständen auch bei einer falsch eingestellten MSN bzw. EAZ!

Bestätigen Sie Ihre Angaben mit dem Schalter „Weiter“ am Ende dieser Seite.

7.2.2. Einrichtung für den Support (ausgehend)

Tragen Sie hier die Rufnummern ein, die für einen eventuellen Supportzugang gewählt werden sollen. Hier können bereits Nummern Ihres Supports (siehe Kapitel 14) hinterlegt sein. Sie sehen zwei fast gleiche Einträge, nur mit dem Unterschied, dass im einem Falle eine „0“ zur Amtsholung (bei Verwendung einer Telefonanlage meist notwendig) zuvor gestellt ist. Wenn Sie wissen, ob eine „0“ benötigt wird oder nicht, kann der markierte nichtzutreffende Eintrag mit Hilfe des Schalters „Entfernen“ gelöscht werden.

> *Hinweis:*
>
> *Alle Einträge auf dieser Seite beziehen sich nur auf ausgehende Anrufe! Vergewissern Sie sich, ob eine „0“ zur Amtsholung benötigt wird. Fragen Sie bei Bedarf den Betreuer Ihrer Telefonanlage.*

Bitte löschen Sie den nicht benötigten Eintrag, da sonst eventuell versucht wird, über diese Rufnummer eine Verbindung herzustellen.

Bestätigen Sie Ihre Eingaben mit Hilfe des Schalters „Weiter“. Somit gelangen Sie in die Maske zur Angabe der eingehenden Rufnummern.

7.2.3. Einrichtung für den Support (eingehend)

Damit ein eingehender Anruf eines Fernwarters akzeptiert wird, können die entsprechenden Nummern hinterlegt werden. Alle sonstigen Rufnummern, die den DEFENDO anrufen und hier nicht hinterlegt sind, werden abgelehnt.

Auch hier können bereits Nummern Ihres Supports (siehe Kapitel 14) hinterlegt sein. Je nach Telefonanlage kann es sein, dass die vorangestellten Nullen durch die Telefonanlage „geschluckt“ werden. Beachten Sie bitte, dass bei einem Anschluss direkt an einen NTBA der Telekom die 0 immer „geschluckt“ wird.

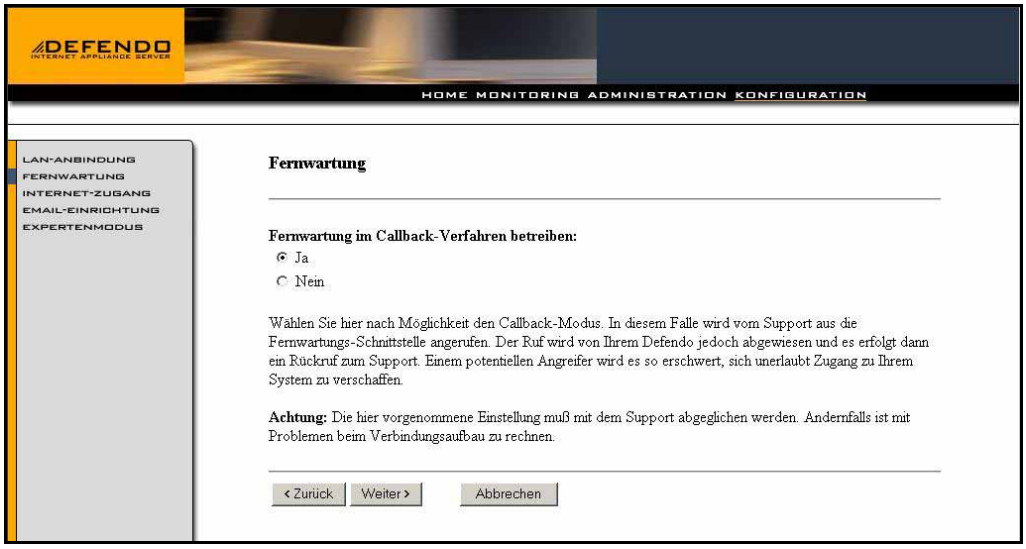
Mit Hilfe des ISDN-Monitors (siehe Kapitel 11.5) können Sie heraus bekommen, welche Rufnummer durch Ihre Telefonanlage übermittelt wird, wenn die Verbindung aktiv ist. Somit können die markierten Einträge die nicht zutreffend sind über den Schalter „Entfernen“ gelöscht werden. Auch hier gilt, die nicht zutreffenden Einträge zu löschen.

Bestätigen Sie Ihre Eingaben mit dem Schalter „Weiter“ am Ende dieser Seite.

7.2.4. Callback-Funktion einrichten

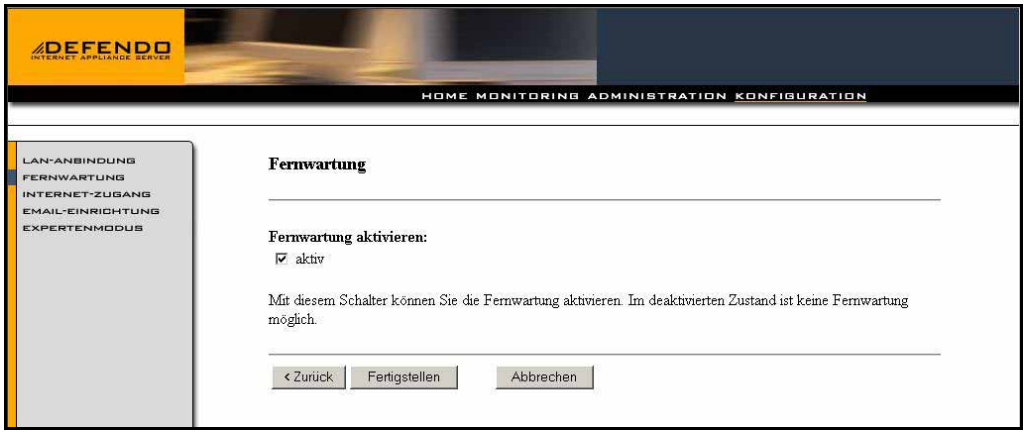
Wählen Sie hier nach Möglichkeit den Callback-Modus. In diesem Falle wird vom Support aus die Fernwartungs-Schnittstelle angerufen. Vom DEFENDO wird dann ein Rückruf initiiert. Einem potentiellen Angreifer wird es so erschwert, sich unerlaubt Zugang zu Ihrem System zu verschaffen.

> *Hinweis:*
>
> *Die hier vorgenommene Einstellung muss mit dem Support (siehe Kapitel 14) abgeglichen werden. Andernfalls ist mit Problemen beim Verbindungsaufbau zu rechnen.*

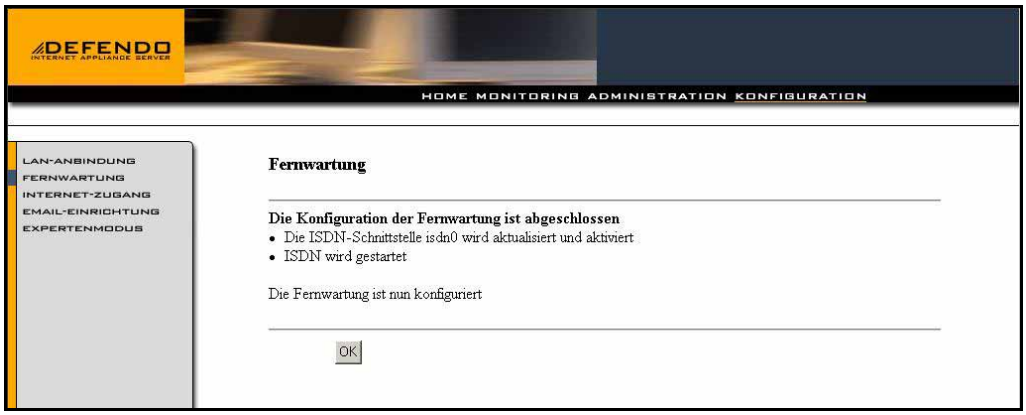

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Fernwartung
Fernwartung im Callback-Verfahren betreiben:
Ja
Nein
Wählen Sie hier nach Möglichkeit den Callback-Modus. In diesem Falle wird vom Support aus die Fernwartungs-Schnittstelle angerufen. Der Ruf wird von Ihrem Defendo jedoch abgewiesen und es erfolgt dann ein Rückruf zum Support. Einem potentiellen Angreifer wird es so erschwert, sich unerlaubt Zugang zu Ihrem System zu verschaffen.
Achtung: Die hier vorgenommene Einstellung muß mit dem Support abgeglichen werden. Andernfalls ist mit Problemen beim Verbindungsaufbau zu rechnen.
< Zurück
Weiter >
Abbrechen

Nachdem alle Einstellungen getätigt wurden, muss der entsprechende Dienst gestartet werden.

Dies erfolgt automatisch, wenn Sie in der darauffolgenden Maske den Schalter „Fertigstellen“ wählen und den Haken bei Fernwartung aktivieren auf „Aktiv“ belassen. Sollten Sie etwaige Änderungen Ihrer Eingaben wünschen oder notwendig seien, so wählen Sie den Schalter „Zurück“.



Nach Anwahl des Schalter „Fertigstellen“ sind die Eingaben in diesem Konfigurations-Assistenten abgeschlossen.



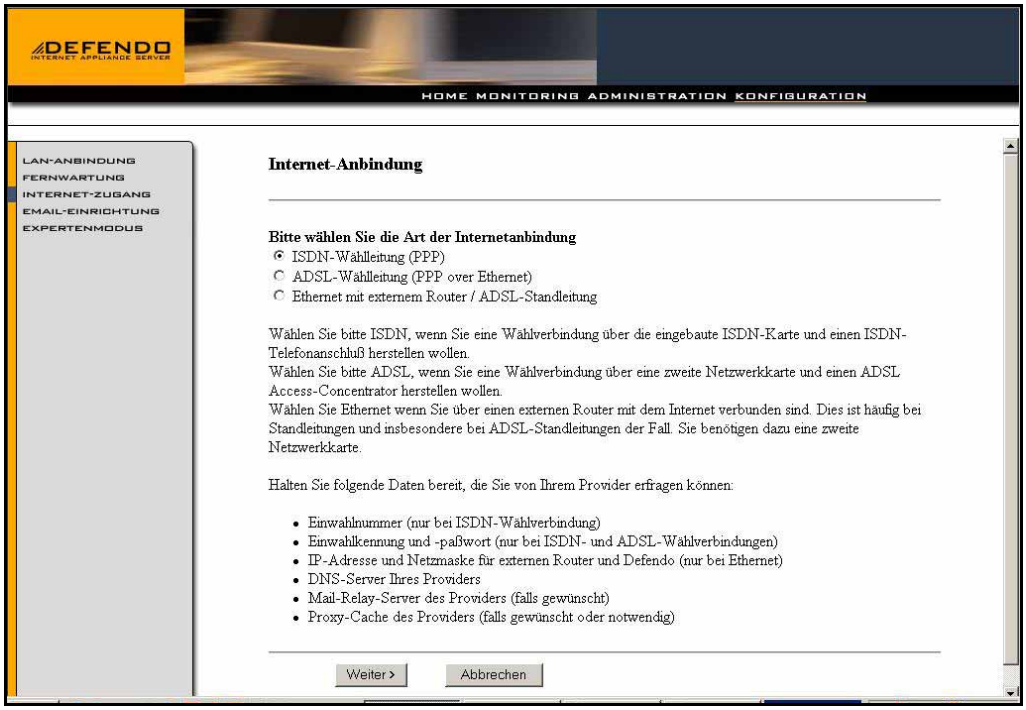
Hinweis:

Bitte rufen Sie Ihren Supports (siehe Kapitel 14) nach diesem Konfigurations-Assistenten an, damit er überprüfen kann, ob die Fernwartung richtig konfiguriert ist. Sollte dies der Fall seien, haben Sie das Schlimmste überstanden. Alle weiteren Einstellungen kann ihr Support nach Ihren Vorgaben gegebenenfalls über die Fernwartung einstellen und konfigurieren. Diese Dienstleistung und Hilfestellungen sind in der Regel kostenpflichtig. Weiter Informationen hierfür erhalten Sie im Kapitel 14 (Support).

7.3. Der Konfigurations-Assistent „Internet-Zugang“

Mit Hilfe dieses Konfigurations-Assistenten können Sie sich schnell und einfach einen Internet-Zugang einrichten, der dann von allen Workstations (Arbeitsplatz-PCs in Ihrem LAN) genutzt werden kann. Es gibt verschiedene Arten der Internetanbindung. Der Konfigurations-Assistent unterstützt Sie, wenn Sie auf eine der folgenden Arten an das Internet angebunden sind:

- ISDN-Wählleitung mit synchronem PPP-Protokoll. Dies ist der Standardzugang zum Internet, der praktisch von jedem Provider angeboten wird.
- ADSL-Wählleitung mit PPP over Ethernet.
- Ethernet-Verbindung über externen Router. Im allgemeinen ist dies der Fall, wenn Sie über eine Standleitung mit Ihrem Provider verbunden sind und der Provider dazu einen Router mit Ethernet-Anschluß bei Ihnen aufgestellt hat. Auch bei ADSL-Standleitungen erhalten Sie normalerweise einen solchen externen Router.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
Bitte wählen Sie die Art der Internetanbindung
ISDN-Wählleitung (PPP)
ADSL-Wählleitung (PPP over Ethernet)
Ethernet mit externem Router / ADSL-Standleitung
Wählen Sie bitte ISDN, wenn Sie eine Wählverbindung über die eingebaute ISDN-Karte und einen ISDN-Telefonanschluß herstellen wollen.
Wählen Sie bitte ADSL, wenn Sie eine Wählverbindung über eine zweite Netzwerkkarte und einen ADSL Access-Concentrator herstellen wollen.
Wählen Sie Ethernet wenn Sie über einen externen Router mit dem Internet verbunden sind. Dies ist häufig bei Standleitungen und insbesondere bei ADSL-Standleitungen der Fall. Sie benötigen dazu eine zweite Netzwerkkarte.
Halten Sie folgende Daten bereit, die Sie von Ihrem Provider erfragen können:
Einwahlnummer (nur bei ISDN-Wählverbindung)
Einwahlkennung und -paßwort (nur bei ISDN- und ADSL-Wählverbindungen)
IP-Adresse und Netzmaske für externen Router und Defendo (nur bei Ethernet)
DNS-Server Ihres Providers
Mail-Relay-Server des Providers (falls gewünscht)
Proxy-Cache des Providers (falls gewünscht oder notwendig)
Weiter >
Abbrechen

Wählen Sie aus der ersten Maske des Internet-Assistenten den Anbindungstyp aus, der für Sie zutrifft und bestätigen Sie Ihre Auswahl mit dem Schalter „Weiter“ am Ende der Seite. Lesen Sie bitte in dem zu Ihrer Anbindungsart gehörenden Kapitel weiter.

7.3.1. Internetanbindung mit ISDN-Wählleitung

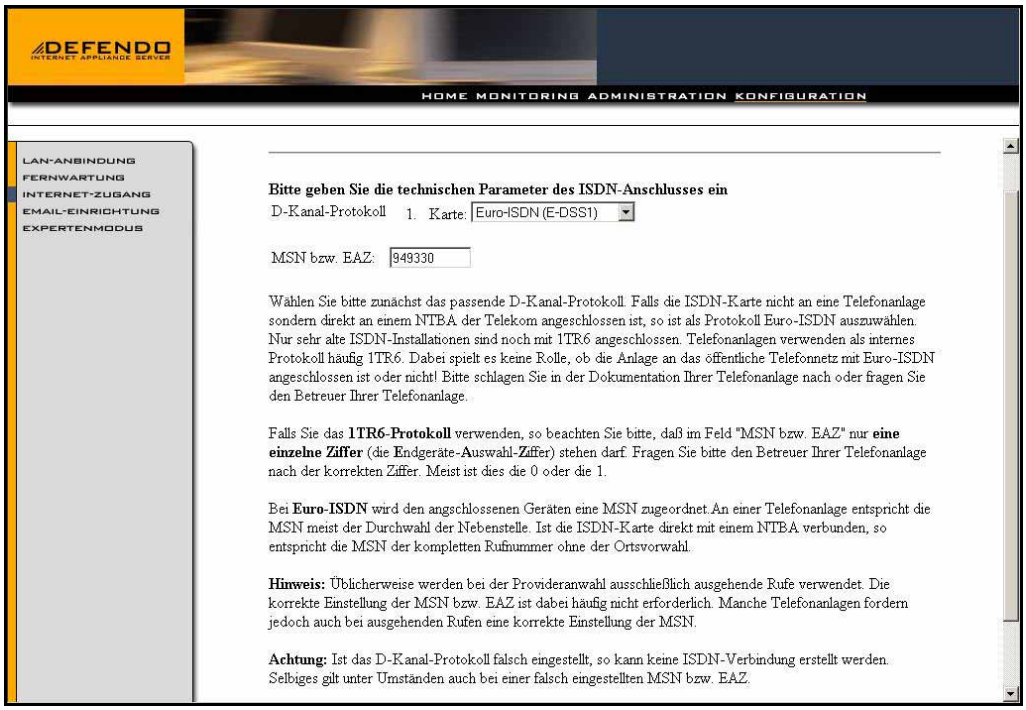
Die Internetanbindung über ISDN-Wählleitung mit synchronem PPP-Protokoll erfolgt über die eingebaute ISDN-Karte des DEFENDO . Verbinden Sie diese mit einem NTBA der Telekom oder mit einem ISDN-S0-Bus Ihrer Telefonanlage. Über den Konfigurations-Assistenten konfigurieren Sie die Schnittstelle ippp0 des DEFENDO .

Folgende Informationen sind für diese Einrichtung notwendig:

- Benötigte Einstellungen für den ISDN-Anschluß (D-Kanal-Protokoll, MSN, Amtsholung)
- Einwahlnummer des Providers (bei T-Online bereits hinterlegt)
- Einwahlkennung und Passwort zur Anmeldung beim Provider
- DNS-Server des Providers (bei T-Online bereits hinterlegt)

- Ggf. Mail-Relay-Server des Providers (bei T-Online bereits hinterlegt)
- Ggf. Proxy-Cache des Providers (bei T-Online nicht notwendig)

Bei der Konfiguration von ISDN-Wählleitungen sind wie auch bereits im Konfigurations-Assistenten “Fernwartung“ erst die Einstellungen für den ISDN-Anschluss zu machen. Verwenden Sie hierfür die gleichen Einträge bei Wahl des D-Kanal Protokolls (Euro, 1TR6, NI1), sowie die entsprechende MSN (bei Euro), EAZ (bei 1TR6) oder MSN:SPID (bei NI1). Wechseln Sie dann mit der „Weiter“-Schaltfläche zur nächsten Maske.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Bitte geben Sie die technischen Parameter des ISDN-Anschlusses ein
D-Kanal-Protokoll 1. Karte: Euro-ISDN (E-DSS1)
MSN bzw. EAZ: 949330
Wählen Sie bitte zunächst das passende D-Kanal-Protokoll. Falls die ISDN-Karte nicht an eine Telefonanlage sondern direkt an einem NTBA der Telekom angeschlossen ist, so ist als Protokoll Euro-ISDN auszuwählen. Nur sehr alte ISDN-Installationen sind noch mit 1TR6 angeschlossen. Telefonanlagen verwenden als internes Protokoll häufig 1TR6. Dabei spielt es keine Rolle, ob die Anlage an das öffentliche Telefonnetz mit Euro-ISDN angeschlossen ist oder nicht! Bitte schlagen Sie in der Dokumentation Ihrer Telefonanlage nach oder fragen Sie den Betreuer Ihrer Telefonanlage.
Falls Sie das 1TR6-Protokoll verwenden, so beachten Sie bitte, daß im Feld "MSN bzw. EAZ" nur eine einzelne Ziffer (die Endgeräte-Auswahl-Ziffer) stehen darf. Fragen Sie bitte den Betreuer Ihrer Telefonanlage nach der korrekten Ziffer. Meist ist dies die 0 oder die 1.
Bei Euro-ISDN wird den angschlossenen Geräten eine MSN zugeordnet.An einer Telefonanlage entspricht die MSN meist der Durchwahl der Nebenstelle. Ist die ISDN-Karte direkt mit einem NTBA verbunden, so entspricht die MSN der kompletten Rufnummer ohne der Ortsvorwahl.
Hinweis: Üblicherweise werden bei der Provideranwahl ausschließlich ausgehende Rufe verwendet. Die korrekte Einstellung der MSN bzw. EAZ ist dabei häufig nicht erforderlich. Manche Telefonanlagen fordern jedoch auch bei ausgehenden Rufen eine korrekte Einstellung der MSN.
Achtung: Ist das D-Kanal-Protokoll falsch eingestellt, so kann keine ISDN-Verbindung erstellt werden. Selbiges gilt unter Umständen auch bei einer falsch eingestellten MSN bzw. EAZ.

Es wird nun abgefragt, ob Sie sich über T-Online oder einen anderen Provider in das Internet einwählen. Selektieren Sie die für Sie zutreffende Option. Mit der „Weiter“-Schaltfläche gelangen Sie zur nächsten Maske. Falls Sie T-Online gewählt haben, lesen Sie bitte im Kapitel 7.3.5 weiter, andernfalls im Kapitel 7.3.4.

7.3.2. Internetanbindung mit ADSL-Wählleitung

Die Internetanbindung über ADSL-Wählleitung und dem PPP-over-Ethernet-Protokoll erfolgt über eine Netzwerk-Karte des DEFENDO . Verbinden Sie diese mit dem Access-Concentrator bzw. ADSL-Modem, das durch Ihren Provider gestellt wird.

Über den Konfigurations-Assistenten konfigurieren Sie die Schnittstelle adsl0 des DEFENDO . Der Konfigurations-Assistent prüft ob die Schnittstellen eth1 bzw. eth2, die mit der zweiten bzw. dritten Netzwerkkarte des Systems korrespondieren als reguläre Ethernet-Schnittstelle konfiguriert sind. Es wird die erste unbenutzte Schnittstelle für die ADSL-Verbindung verwendet. Sind sowohl eth1 als auch eth2 als Ethernet benutzt, so wird eth3 (die vierte Netzwerkkarte) für ADSL konfiguriert.

> *Hinweis:*
>
> *Der DEFENDO muß über eine eigene Netzwerkkarte für ADSL verfügen. Diese darf nicht bereits als Ethernet-Schnittstelle in Verwendung sein. Sollte eine der Netzwerkkarten fälschlicherweise bereits als Ethernet-Schnittstelle konfiguriert sein, so löschen Sie diese bitte zunächst (vgl. Kapitel 12.1.1)*

Folgende Informationen sind für diese Einrichtung notwendig:

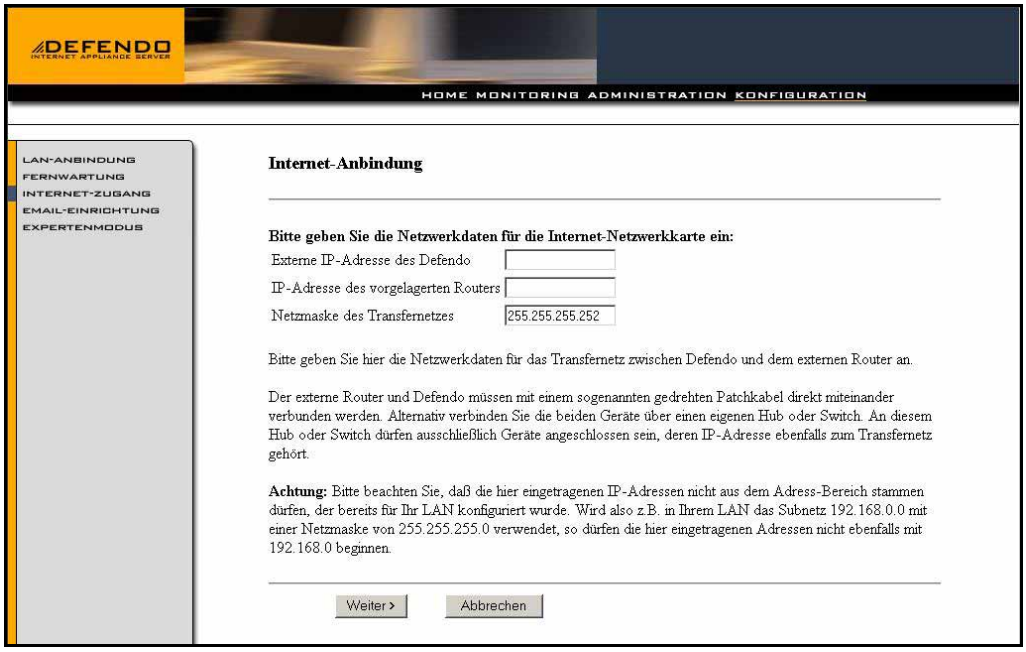
- Einwahlkennung und Passwort zur Anmeldung beim Provider
- DNS-Server des Providers (bei T-Online bereits hinterlegt)
- Ggf. Mail-Relay-Server des Providers (bei T-Online bereits hinterlegt)
- Ggf. Proxy-Cache des Providers (bei T-Online nicht notwendig)

Bei der Konfiguration von ADSL-Wählleitungen wird zunächst abgefragt, ob Sie sich über T-DSL (T-Online) oder einen anderen Provider in das Internet einwählen. Selektieren Sie die für Sie zutreffende Option. Mit der „Weiter“-Schaltfläche gelangen Sie zur nächsten Maske. Falls Sie T-Online gewählt haben, lesen Sie bitte im Kapitel 7.3.5 weiter, andernfalls im Kapitel 7.3.4.

7.3.3. Internetanbindung über Ethernet-Router

Eine Internetanbindung über einen externen Router ist häufig dann der Fall, wenn Sie an eine Standleitung angeschlossen sind (insbesondere auch bei ADSL-Standleitungen). Ein anderes denkbares Szenario wäre der Anschluß an eine vorgeschaltete Firewall oder auch an einen Wählleitungs-Router. In jedem Falle darf die externe Schnittstelle des DEFENDO nicht eine IP-Adresse aus dem IP-Kreis Ihres LANs erhalten. Es muß ein eigenes IP-Subnetz zwischen dem DEFENDO und dem externen Router erstellt werden. Bei Standleitungen erhalten Sie die Daten zu diesem Transfernetz von Ihrem Provider. Es handelt sich dabei meist um feste Internet IP-Adressen, die ausschließlich Ihrem

Transfernetz zugeordnet sind und als solche auch jederzeit von jedermann im Internet angesprochen werden können.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
Bitte geben Sie die Netzwerkdaten für die Internet-Netzwerkkarte ein:
Externe IP-Adresse des Defendo
IP-Adresse des vorgelagerten Routers
Netzmaske des Transfernetzes
255.255.255.252
Bitte geben Sie hier die Netzwerkdaten für das Transfernetz zwischen Defendo und dem externen Router an.
Der externe Router und Defendo müssen mit einem sogenannten gedrehten Patchkabel direkt miteinander verbunden werden. Alternativ verbinden Sie die beiden Geräte über einen eigenen Hub oder Switch. An diesem Hub oder Switch dürfen ausschließlich Geräte angeschlossen sein, deren IP-Adresse ebenfalls zum Transfernetz gehört.
Achtung: Bitte beachten Sie, daß die hier eingetragenen IP-Adressen nicht aus dem Adress-Bereich stammen dürfen, der bereits für Ihr LAN konfiguriert wurde. Wird also z.B. in Ihrem LAN das Subnetz 192.168.0.0 mit einer Netzmaske von 255.255.255.0 verwendet, so dürfen die hier eingetragenen Adressen nicht ebenfalls mit 192.168.0 beginnen.
Weiter >
Abbrechen

Für die Kommunikation mit dem externen Router muß eine noch nicht anderweitig benutzte Netzwerkkarte des DEFENDO mit dem externen Router verbunden werden. Verwenden Sie ein gekreuztes Patchkabel (Crossover-Kabel) um die Netzwerkkarte des DEFENDO direkt mit dem Netzwerkanschluß des externen Routers zu verwenden. Ein gekreuztes Patchkabel ist nicht im Lieferumfang enthalten. Alternativ können Sie DEFENDO und den Router über einen dazwischengeschalteten Hub oder Switch verbinden. Bitte beachten Sie, daß Sie für dieses externe Netzwerk einen eigenen Hub oder Switch benötigen und nicht den Hub oder Switch verwenden können, an dem z.B. Rechner aus Ihrem LAN angeschlossen sind. An diesem externen Hub oder Switch dürfen neben dem DEFENDO und dem externen Router ausschließlich Geräte angeschlossen werden, die IP-technisch zum gleichen Netzwerk wie Router und DEFENDO gehören.

Über den Konfigurations-Assistenten konfigurieren Sie die Schnittstelle eth1 des DEFENDO . Sollte die ADSL-Schnittstelle adsl0 bereits eth1 verwenden, so wird adsl0 zu Benutzung von eth2 bzw. eth3 umkonfiguriert.

Hinweis:

Der DEFENDO muß über eine eigene Netzwerkkarte für die Internetanbindung über Ethernet-Router verfügen.

Folgende Informationen sind für diese Einrichtung notwendig:

- IP-Adresse des externen Routers
- IP-Adresse des DEFENDO
- Netzmaske des Transfernetzes zwischen DEFENDO und Router
- DNS-Server des Providers
- Ggf. Mail-Relay-Server des Providers
- Ggf. Proxy-Cache des Providers

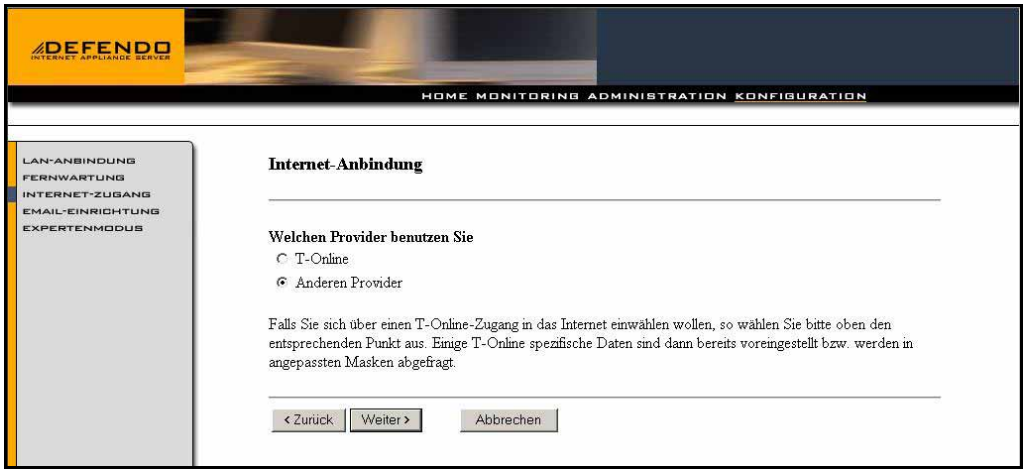
Zunächst werden nun die IP-Daten für das Transfernetz zwischen DEFENDO und externem Router abgefragt. Tragen Sie die externe IP-Adresse des DEFENDO , die (interne) IP-Adresse des Routers und die zugehörige Netzmaske ein. Lautet die Netzmaske die Sie von Ihrem Provider erhalten haben 255.255.255.252, so gibt es keine Möglichkeit weitere Geräte an das Transfernetz anzuschließen. DEFENDO und Router können direkt mit einem gekreuzten Patchkabel miteinander verbunden werden. Bei anderen Netzmasken ist es möglich, weitere Geräte in dem Transfernetz anzuschließen (z.B. Web-Server, Mail-Server, ...) wenn für das Transfernetz ein eigener Hub oder Switch zur Verfügung steht. Auf diese Server ist dann meist der direkte aber ungeschützte Zugriff aus dem Internet möglich. Nähere Auskünfte dazu erhalten Sie von Ihrem Provider.

Achtung:

Die IP-Adresse für die externe Schnittstelle des DEFENDO darf nicht Bestandteil des IP-Kreises sein, der für Ihr LAN vorgesehen ist.

Verbinden Sie die externe Schnittstelle des DEFENDO und den externen Router nie über einen Hub oder Switch, an dem auch Geräte aus dem LAN angeschlossen sind.

Klicken Sie auf die „Weiter“-Schaltfläche am Ende der Seite um mit der nächsten Maske fortzufahren.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
Welchen Provider benutzen Sie
T-Online
Anderen Provider
Falls Sie sich über einen T-Online-Zugang in das Internet einwählen wollen, so wählen Sie bitte oben den entsprechenden Punkt aus. Einige T-Online spezifische Daten sind dann bereits voreingestellt bzw. werden in angepassten Masken abgefragt.
< Zurück
Weiter >
Abbrechen

7.3.4. Internet-Zugang über „andere Provider“

Die weitere Konfiguration ist für die Internetanbindung mit ISDN-Wählleitung, ADSL-Wählleitung oder externen Router (Standleitung) weitgehend gleich. Auf Unterschiede wird jeweils hingewiesen.

7.3.4.1. Einwahldaten eingeben

Sollten Sie über Ethernet an einen externen Router angebunden sein, so können Sie diesen Abschnitt überspringen.

Geben Sie hier bitte die anzuwählende Telefonnummer (fehlt bei ADSL), sowie Benutzername und Kennwort für die Einwahl bei Ihrem Provider ein. Sollten Sie von Ihrem Provider mehrere Kennungen erhalten haben (z.B. auch für E-Mail / POP3 und für die Pflege Ihres Web-Servers), so verwenden Sie bitte die Kennung für PPP, PAP oder CHAP. Alle benötigten Eingaben bekommen Sie bzw. haben Sie bereits von Ihren Provider bekommen:

> *Hinweis:*
>
> *Bitte vergessen Sie bei ISDN-Wählverbindungen nicht, der Telefonnummer die Amtsholung der Telefonanlage voranzustellen, sofern dies erforderlich ist.*

- **Rufnummer (fehlt bei ADSL)**
  Tragen Sie hier bitte die entsprechen Rufnummer Ihres Providers ein. Bitte beachten Sie, daß bei Verwendung einer Telefonanlage eventuell eine „0“ oder eine andere Vorwahlnummer zum Erhalt einer Amtsleitung notwendig ist.
- **Benutzername**
  Verwenden Sie hier die entsprechende Benutzerkennung zum Zugang des Internets über Ihren Provider.
- **Kennwort**
  Von Ihrem Provider wurde Ihnen ein Zugangspasswort zugeteilt. Bitte tragen Sie dieses in dieses Feld ein.

Bestätigen Sie Ihre Eingaben mit Schalter „Weiter“ am Ende dieser Seite.

7.3.4.2. Der DNS-Server Ihre Providers

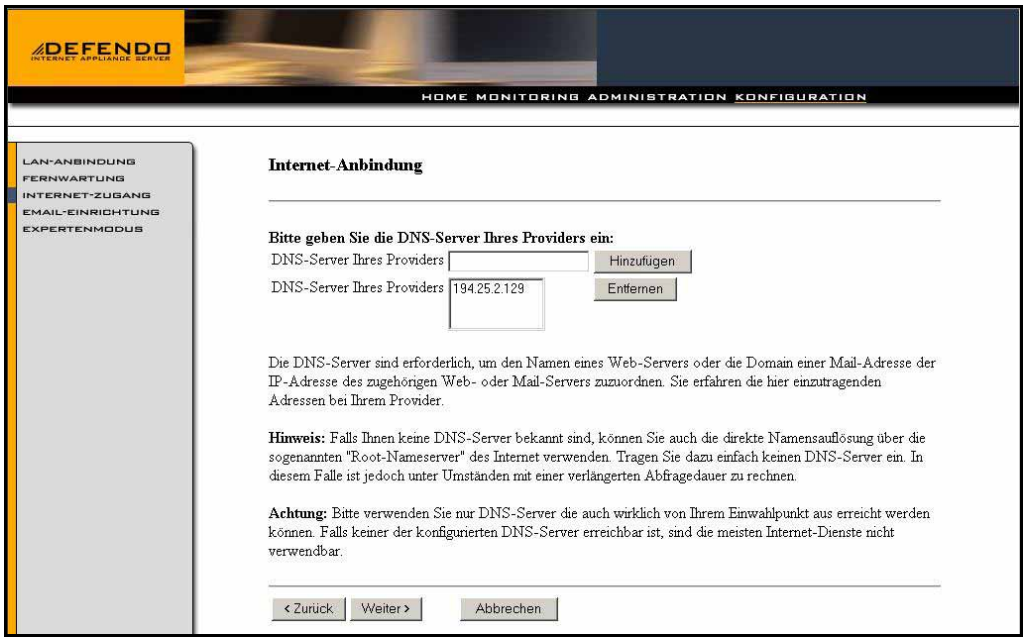
Nun wird der DNS-Server (falls vorhanden) Ihres Providers abgefragt. Die DNS-Server sind erforderlich, um den Namen eines Web-Servers oder die Domain einer Mail-Adresse der IP-Adresse des zugehörigen Web- oder Mail-Servers zuzuordnen. Sie erfahren die hier einzutragenden Adressen bei Ihrem Provider.

Hinweis:

Falls Ihnen keine DNS-Server bekannt sind, können Sie auch die direkte Namensauflösung über die sogenannten „Root-Nameserver“ des Internet verwenden. Tragen Sie dazu einfach keinen DNS-Server ein. In diesem Falle ist jedoch unter Umständen mit einer verlängerten Abfragedauer zu rechnen.

Bitte verwenden Sie nur DNS-Server die auch wirklich von Ihrem Einwahlpunkt aus erreicht werden können. Falls keiner der konfigurierten DNS-Server erreichbar ist, sind die meisten Internet-Dienste nicht verwendbar.

Tragen Sie bitte den DNS-Server Ihres Providers in die nachfolgende Maske ein:

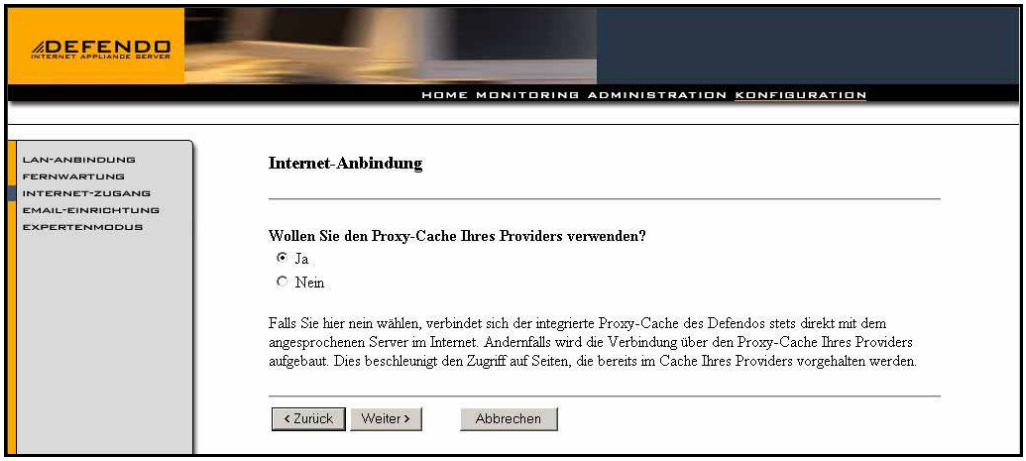

DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
Bitte geben Sie die DNS-Server Ihres Providers ein:
DNS-Server Ihres Providers
Hinzufügen
DNS-Server Ihres Providers
194.25.2.129
Entfernen
Die DNS-Server sind erforderlich, um den Namen eines Web-Servers oder die Domain einer Mail-Adresse der IP-Adresse des zugehörigen Web- oder Mail-Servers zuzuordnen. Sie erfahren die hier einzutragenden Adressen bei Ihrem Provider.
Hinweis: Falls Ihnen keine DNS-Server bekannt sind, können Sie auch die direkte Namensauflösung über die sogenannten "Root-Nameserver" des Internet verwenden. Tragen Sie dazu einfach keinen DNS-Server ein. In diesem Falle ist jedoch unter Umständen mit einer verlängerten Abfragedauer zu rechnen.
Achtung: Bitte verwenden Sie nur DNS-Server die auch wirklich von Ihrem Einwahlpunkt aus erreicht werden können. Falls keiner der konfigurierten DNS-Server erreichbar ist, sind die meisten Internet-Dienste nicht verwendbar.
< Zurück
Weiter >
Abbrechen

Um Ihrem Eintrag hinzuzufügen, betätigen Sie bitte den Schalter „Hinzufügen“. Ihre Eingaben werden mit dem Schalter „Weiter“ am Ende dieser Seite übernommen.

7.3.4.3. Der Proxy-Cache-Server des Providers

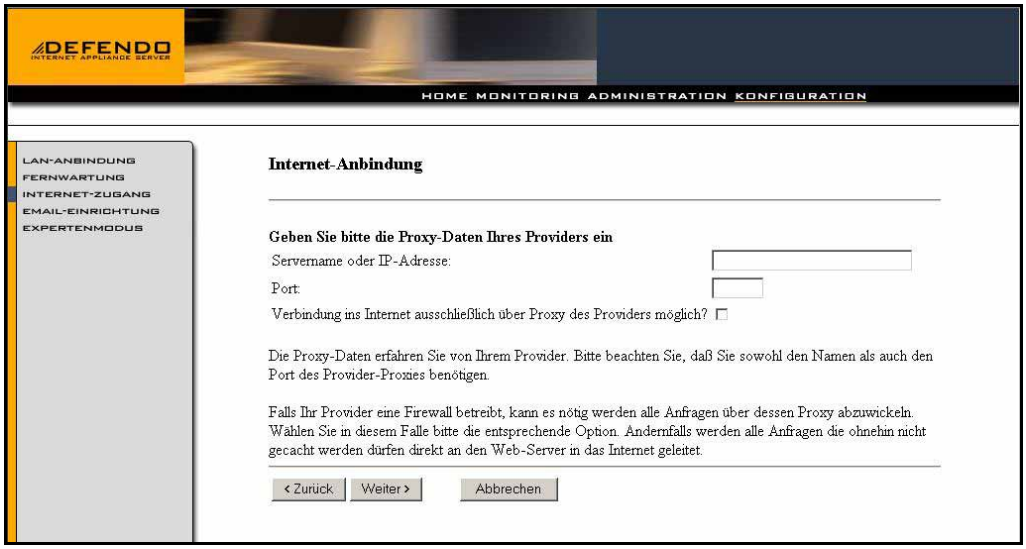
Es wird nun zur Abfrage des Proxy-Cache-Servers gewechselt. Wenn gewünscht bzw. verfügbar, kann der DEFENDO einen von Ihrem Provider zur Verfügung gestellten Proxy-Cache verwenden. Sollte Ihr Provi-

der keinen Proxy-Cache-Server zur Verfügung stellen, oder Sie diesen nicht nützen wollen, verbindet der DEFENDO immer direkt mit der angesprochenen Adresse. Der DEFENDO fungiert selbst als eigener Proxy-Cache-Server.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
Wollen Sie den Proxy-Cache Ihres Providers verwenden?
Ja
Nein
Falls Sie hier nein wählen, verbindet sich der integrierte Proxy-Cache des Defendos stets direkt mit dem angesprochenen Server im Internet. Andernfalls wird die Verbindung über den Proxy-Cache Ihres Providers aufgebaut. Dies beschleunigt den Zugriff auf Seiten, die bereits im Cache Ihres Providers vorgehalten werden.
< Zurück
Weiter >
Abbrechen

Sollten Sie den Proxy-Cache-Server Ihres Providers nicht nutzen wollen, so wählen Sie den Eintrag „Nein“. In diesem Fall verbindet sich der integrierte Proxy-Cache des DEFENDO stets direkt mit dem angesprochenen Adresse im Internet. Fahren Sie in diesem Fall im Kapitel 7.3.4.4 fort. Andernfalls wird die Verbindung über den Proxy-Cache Ihres Providers aufgebaut. Dies beschleunigt den Zugriff auf Seiten, die bereits im Cache Ihres Providers vorgehalten werden.

Wenn Sie den Proxy-Cache-Server Ihres Provider verwenden wollen, so wählen Sie bitte den Schalter „Weiter“. Es wird nun in die Eingabemaske der Proxy-Cache-Einstellungen gewechselt.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
Geben Sie bitte die Proxy-Daten Ihres Providers ein
Servername oder IP-Adresse:
Port:
Verbindung ins Internet ausschließlich über Proxy des Providers möglich?
Die Proxy-Daten erfahren Sie von Ihrem Provider. Bitte beachten Sie, daß Sie sowohl den Namen als auch den Port des Provider-Proxies benötigen.
Falls Ihr Provider eine Firewall betreibt, kann es nötig werden alle Anfragen über dessen Proxy abzuwickeln. Wählen Sie in diesem Falle bitte die entsprechende Option. Andernfalls werden alle Anfragen die ohnehin nicht gecacht werden dürfen direkt an den Web-Server in das Internet geleitet.
< Zurück
Weiter >
Abbrechen

Tragen Sie bitte in die entsprechenden Felder die Angaben zum Proxy-Cache-Server Ihres Providers ein. Bitte beachten Sie, dass Sie sowohl den Namen als auch den Port des Proxy-Cache-Servers Ihres Providers benötigen.

Falls Ihr Provider eine entsprechend reglementierte Firewall betreibt, kann es nötig werden, alle Anfragen über dessen Proxy-Cache-Server abzuwickeln. Wählen Sie in diesem Falle bitte die entsprechende Option. Andernfalls werden alle Anfragen, die ohnehin nicht in einem Cache gespeichert werden dürfen, direkt an den Web-Server in das Internet geleitet. Lediglich Anfragen, die möglicherweise im Cache des Providers liegen können, werden auch in diesen gestellt.

Bestätigen Sie Ihre Angaben mit den Schalter „Weiter“. Somit haben Sie die Einstellungen abgeschlossen.

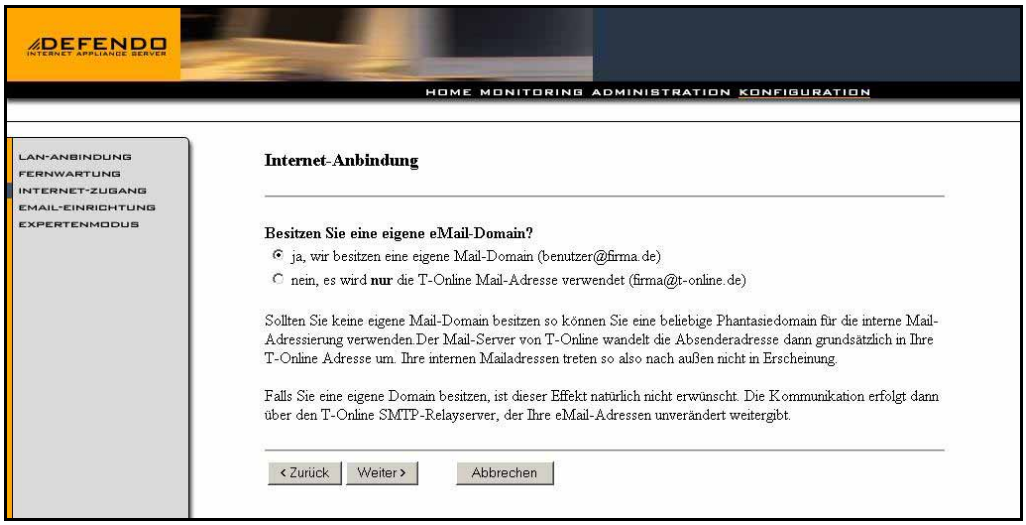
7.3.4.4. Mailserver des Providers

Ausgehende Mails können entweder direkt an den E-Mail-Server des Empfängers oder zunächst an den E-Mail-Server Ihres Providers versendet werden.

Letzteres empfiehlt sich insbesondere bei Wählverbindungen, da die E-Mail so recht schnell die teuere Wählleitung passiert. Ferner wird die E-Mail dann selbst im Fehlerfall nur einmal übermittelt.

Ist hingegen der direkte Versand eingestellt und der E-Mail-Server des Empfängers nicht erreichbar, wird versucht die E-Mail in bestimmten zeitlichen Abständen erneut zuzustellen, wobei bei Wählverbindungen

wiederum Verbindungskosten anfallen. Bei Standleitungen wird häufig der direkte Versand gewählt, da im Falle einer fehlerhaften Verbindung dies über das Monitoring jederzeit direkt überprüft werden kann.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
Besitzen Sie eine eigene eMail-Domain?
ja, wir besitzen eine eigene Mail-Domain (benutzer@firma.de)
nein, es wird nur die T-Online Mail-Adresse verwendet (firma@t-online.de)
Sollten Sie keine eigene Mail-Domain besitzen so können Sie eine beliebige Phantasiedomain für die interne Mail-Adressierung verwenden.Der Mail-Server von T-Online wandelt die Absenderadresse dann grundsätzlich in Ihre T-Online Adresse um. Ihre internen Mailadressen treten so also nach außen nicht in Erscheinung.
Falls Sie eine eigene Domain besitzen, ist dieser Effekt natürlich nicht erwünscht. Die Kommunikation erfolgt dann über den T-Online SMTP-Relayserver, der Ihre eMail-Adressen unverändert weitergibt.
< Zurück
Weiter >
Abbrechen

Wird Ihnen ein Mail-Relay vom Provider zur Verfügung gestellt und Sie wollen diesen Dienst nützen, so wählen Sie bitte die Schaltbox „Ja“, andernfalls „Nein“. Bestätigen Sie ihre Auswahl mit dem Schalter „Weiter“. Wenn Sie das Mail-Relay nicht nutzen wollen lesen Sie bitte in Kapitel 7.3.6 weiter.

In der nachfolgenden Maske wird nun der Name oder die IP-Adresse des E-Mail-Servers Ihres Providers abgefragt („Servername oder IP-Adresse:“). Bitte tragen Sie diesen Wert exakt in das entsprechende Feld ein. Diesen Wert erhalten Sie bei Ihrem Provider.

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
T-Online SMTP-Relay freischalten
Bei Verwendung einer eigenen Mail-Domain müssen Sie sich zunächst beim Mail-Relayserver von T-Online anmelden. Dazu muß die Browserkommunikation mit dem Internet bereits hergestellt sein. Sollte dies noch nicht der Fall sein, so führen Sie die nachfolgenden Schritte bitte aus, sobald Sie auf Internetseiten zugreifen können.
1. Gehen Sie auf http://www.t-online.de (Dieser Link öffnet ein neues Browser-Fenster)
2. Wählen Sie aus dem Menü auf der linken Seite den Punkt Kundencenter an
3. In der Rubrik Anmeldungen für weitere Dienste wählen Sie dann den Punkt SMTP-Relayserver
4. Melden Sie sich nun an und schalten Sie den Zugang frei.
< Zurück
Weiter >
Abbrechen

Der gesamte Mailverkehr, der nicht für Ihren internen Mail-Server bestimmt ist, wird über den hier eingetragenen Server Ihres Providers abgewickelt. Dieser kümmert sich auch um die Zustellung an den Mail-Server des Empfängers. Im Rahmen seiner Konfiguration versucht dieser auch bei fehlerhaften Verbindungen die Mails später erneut zuzustellen.

Ihre Angabe werden mit dem Schalter „Weiter“ bestätigt. Fahren Sie bitte in Kapitel 7.3.6 fort.

7.3.5. Internet-Zugang über T-Online Wählleitungen

Die nachfolgenden Eingabemasken sind für ISDN- und ADSL-Zugänge fast identisch. Sie erhalten hier die Möglichkeit in einer angepassten Maske T-Online spezifische Einstellungen anzugeben. Andere Einstellungen sind bereits fest voreingestellt. So wird als DNS-Server die Adresse 194.25.2.129 verwendet. Der Proxy-Cache des DEFENDO nutzt keinen übergeordneten Proxy.

7.3.5.1. T-Online Zugangsdaten

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Internet-Anbindung
Bitte geben Sie die Zugangsdaten für die Einwahl bei Ihrem Provider ein:
Rufnummer:
Benutzername:
Kennwort:
Geben Sie hier bitte die anzuwählende Telefonnummer, sowie Benutzername und Kennwort für die Einwahl bei Ihrem Provider ein. Sie erfahren diese Daten bei Ihrem Provider. Sollten Sie von Ihrem Provider mehrere Kennungen erhalten haben (z.B. auch für eMail / POP3 und für die Pflege Ihres Web-Servers), so verwenden Sie bitte die Kennung für PPP, PAP oder CHAP.
Achtung: Bitte vergessen Sie nicht, der Telefonnummer die Amtsholung der Telefonanlage voranzustellen, falls dies erforderlich ist.
< Zurück
Weiter >
Abbrechen

Mit Ihrer Bestätigung für den T-Online-Zugang erhielten Sie von der Telekom AG einen Schreiben. Dieses ist für Eintragungen in dieser Maske notwendig.

Tragen Sie in den entsprechenden Feldern bitte folgendes ein:

- **ggf. Amtholung der Telefonanlage (entfällt bei ADSL)**
  Tragen Sie hier bitte die Ziffer ein, die zur Amtsholung Ihrer Telefonanlage benötigt wird. Dies ist in der Regel die „0“.
- **Anschlusskennung**
  Aus Ihrem Schreiben von der Telekom AG ist diese 12 stellige Kennung ersichtlich. Bitte übertragen Sie diese exakt in dieses Feld.
- **Teilnehmernummer / T-Online-Nummer**
  Diese Nummer entnehmen Sie bitte auch aus dem Schreiben der Telekom AG mit Ihren Zugangsdaten. Sollte die Teilnehmernummer bzw. T-Online-Nummer aus weniger als 12 Ziffern bestehen, wird automatisch das Zeichen # angehängt.
- **Mitbenutzer (Suffix)**
  Tragen Sie hier bitte den entsprechen Mitbenutzersuffix ein. Im Normalfall ist dies 0001.

- **Passwort**

  Standardmäßig ist dieses Passwort ein Zifferncode. Auch dieses finden Sie in Ihrem Schreiben der Telekom AG. Sollten Sie zwischenzeitlich aus Sicherheitsgründen das Passwort verändert haben, so ist hier natürlich das neue Passwort einzutragen.

Sobald alle Eingaben gemacht wurden, kann diese Maske mit dem Schalter „Weiter“ gespeichert und fortgefahren werden. Der DEFENDO fragt nun in der darauffolgenden Maske die Konfiguration Ihrer E-Mail-Adresse oder internen E-Mail-Domain ab.

Sollten Sie keine eigene Mail-Domain besitzen, denken Sie sich eine beliebige Phantasiedomain für Ihre interne Mail-Adressierung aus. Das in diesem Falle benutzte T-Online Mail-Relay mailto.btx.dtag.de wandelt die Absenderadresse aller ausgehenden Mails in Ihre T-Online Adresse um. Ihre internen Mailadressen bleiben so nach außen unsichtbar.

Falls Sie eine eigene Domain besitzen, ist dieser Effekt natürlich nicht erwüscht. Die Kommunikation erfolgt dann über den T-Online „SMTP-Relayserver“, der Ihre E-Mail-Adressen unverändert weitergibt. Wählen Sie hierzu den Eintrag „ja, wir besitzen eine eigene Mail-Domain (benutzer@firma.de)“. Sollte dies nicht der Fall sein, so wählen Sie bitte den Eintrag „nein, es wird nur die T-Online-Mail-Adresse verwendet (firma@t-online.de)“ und fahren Sie im Kapitel 7.3.6 fort.

7.3.5.2. E-Mail-Account über „eigene Domain“

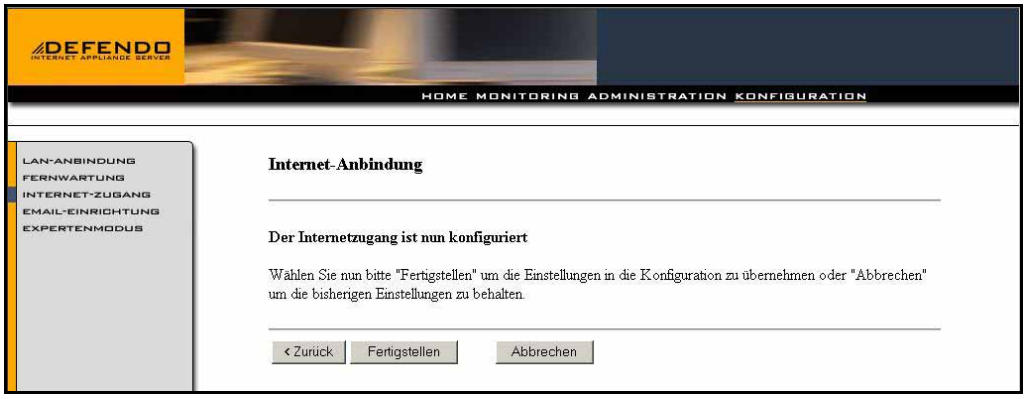
Bei Verwendung einer eigenen Mail-Domain müssen Sie sich zunächst beim Mail-Relayserver von T-Online anmelden. Dazu muss die Browserkommunikation mit dem Internet bereits hergestellt sein. Sollte dies noch nicht der Fall sein, so führen Sie die nachfolgenden Schritte bitte aus, sobald Sie auf Internetseiten zugreifen können.

- Gehen Sie auf http://www.t-online.de .
- Wählen Sie aus dem linken Menü den Bereich **Kundencenter.**
- In der Rubrik **Anmeldung für weitere Dienste** wählen Sie dann den Punkt **SMTP-Relayserver.**
- Melden Sie sich hier an und schalten Sie den Dienst frei.

Der Mail-Versand in das Internet erfolgt über den Server smtprelay.t-online.de.

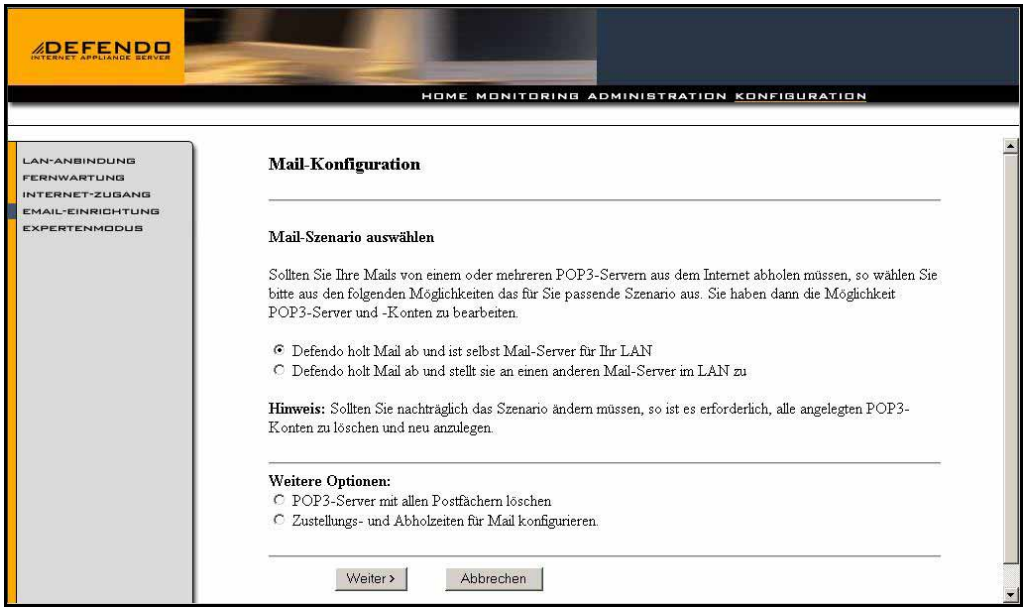
7.3.6. Internet-Zugang fertigstellen

Hiermit sind die Einstellungen im Konfigurations-Assistenten „Internet-Zugang“ abgeschlossen. Eine entsprechende Abschlussmaske betätigt Ihnen dies und verlangt von Ihnen die Speicherung und Aktivierung der Konfiguration mit Hilfe des Schalter „Fertigstellen“. Alle benötigten Dienste werden nun gestartet und auf automatischen Betrieb geschaltet. Alle Angaben können selbstverständlich auch jederzeit über den Konfigurations-Assistenten oder den Menüpunkt Administration bzw. Expertenmodus geändert oder erweitert werden.



7.4. Der Konfigurations-Assistent „eMail-Einrichtung“

Bei der Einrichtung von eMail-Einstellungen werden Sie von diesem Konfigurations-Assistenten unterstützt. Auch er führt Sie Schritt für Schritt durch Masken, in denen Sie die benötigten Informationen eingeben können.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Mail-Szenario auswählen
Sollten Sie Ihre Mails von einem oder mehreren POP3-Servern aus dem Internet abholen müssen, so wählen Sie bitte aus den folgenden Möglichkeiten das für Sie passende Szenario aus. Sie haben dann die Möglichkeit POP3-Server und -Konten zu bearbeiten.
Defendo holt Mail ab und ist selbst Mail-Server für Ihr LAN
Defendo holt Mail ab und stellt sie an einen anderen Mail-Server im LAN zu
Hinweis: Sollten Sie nachträglich das Szenario ändern müssen, so ist es erforderlich, alle angelegten POP3-Konten zu löschen und neu anzulegen.
Weitere Optionen:
POP3-Server mit allen Postfächern löschen
Zustellungs- und Abholzeiten für Mail konfigurieren.
Weiter >
Abbrechen

Sollten Sie Ihre Mails von einem oder mehreren POP3-Servern aus dem Internet abholen müssen, so wählen Sie bitte aus den folgenden Möglichkeiten das für Sie passende Szenario aus. Sie haben dann die Möglichkeit POP3-Server und -Konten zu bearbeiten.

> *Hinweis:*
>
> *Sollten Sie nachträglich das Szenario ändern müssen, so ist es erforderlich, alle angelegten POP3-Konten der POP-Server des Providers zu löschen und neu anzulegen. Die auf dem DEFENDO angelegten POP-Konten müssen nicht neu angelegt werden.*

7.4.1. DEFENDO ist selbst Mail-Server für Ihr LAN

In diesem Fall fungiert der DEFENDO als eMail-Server innerhalb Ihres LANs und holt externe eMails von Ihrem Provider ab. Diese Mails können dann wiederum mit den verschiedensten POP3-Clients (z. B. MS-Outlook) vom DEFENDO abgeholt werden.

7.4.1.1. Mail Domains eintragen

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Vom Defendo Mail-Server verwaltete Domains
Domain
Hinzufügen
kunde.de
Entfernen
Tragen Sie hier alle Domains ein, die vom Mail-Server des Defendo verwaltet werden sollen. Alle Mails, die an eine dieser Domains gerichtet sind, werden nicht in das Internet weitergeleitet sondern in ein lokales Postfach zugestellt.
Richten Sie dazu bitte entsprechende Mail-Verteiler und Benutzer-Konten mit Mail-Berechtigung ein.
Hinweis: Selbstverständlich haben Sie die Möglichkeit, mit Hilfe von Verteilregeln eMail an bestimmte Empfänger innerhalb der obigen Domains an externe Adressen im Internet weiterzuleiten.
Weiter >
Abbrechen

Tragen Sie hier alle Domains ein, die vom Mail-Server des DEFENDO verwaltet werden sollen. Alle Mails, die an eine dieser Domains gerichtet sind, werden ***nicht*** in das Internet weitergeleitet sondern in ein lokales Postfach zugestellt. Richten Sie dazu bitte entsprechende Mail-Verteiler und Benutzer-Konten mit Mail-Berechtigung ein.

> *Hinweis:*
>
> *Selbstverständlich haben Sie die Möglichkeit, mit Hilfe von Verteilregeln E-Mail an bestimmte Empfänger innerhalb der obigen Domains an externe Adressen im Internet weiterzuleiten.*

Zum Eintragen der Domains wählen Sie bitte das freie Eingabefeld und bestätigen Sie Ihre Angaben mit den Schalter „Hinzufügen“. Über „Entfernen“ kann ein selektierter Eintrag auch jederzeit wieder gelöscht werden.

Sind alle Domains eingetragen, wird über den Schalter „Weiter“ am Ende der Seite in die nächste Konfigurationsmaske gewechselt.

7.4.1.2. Virenscanner aktivieren

Die nächste Abfrage in diesem Szenario betrifft die Verwendung des Viren-Scanners beim Eingang von eMails.

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Alle Mails auf Viren prüfen?
Virenscanner aktivieren
Aktivieren Sie diese Option, wenn alle Mails, die den Defendo Mail-Server passieren, auf Viren überprüft werden sollen.
Hinweis: Diese Funktion kann erst genutzt werden, wenn ein Virenscanner auf dem Defendo installiert ist. Die Lizenzen für den Virenscanner sind nicht im Defendo enthalten und müssen separat erworben werden.
< Zurück
Weiter >
Abbrechen

Aktivieren Sie diese Option, wenn ein- und ausgehende eMails, die den Mail-Server des DEFENDO passieren, auf Viren überprüft werden sollen.

> *Hinweis:*
>
> *Diese Funktion kann erst genutzt werden, wenn ein Virenscanner auf dem DEFENDO installiert ist. Die Lizenzen für den Virenscanner sind nicht im DEFENDO enthalten und müssen separat erworben werden. Siehe hierzu auch Kapitel 12.11.*

Bestätigen Sie Ihre Angabe bitte mit den Schalter „Weiter“ am Ende dieser Seite.

7.4.1.3. POP3-Server bearbeiten

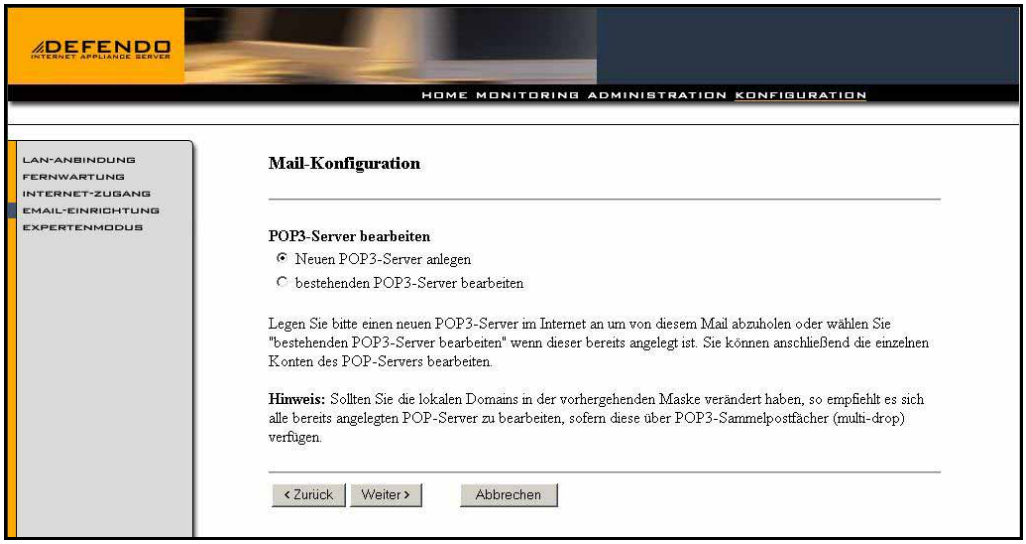
Legen Sie bitte einen neuen POP3-Server im Internet an, um von diesem Mails abzuholen, oder wählen Sie „bestehenden POP3-Server be-

arbeiten“ wenn dieser bereits angelegt ist. Sie können anschließend die einzelnen Konten des POP-Servers bearbeiten.

> *Hinweis:*
>
> *Sollten Sie die lokalen Domains in der ersten Maske verändert haben, so empfiehlt es sich alle bereits angelegten POP-Server zu bearbeiten, sofern diese über POP3-Sammelpostfächer (multi-drop) verfügen.*

Für die Anlage eines neuen POP3-Servers sind Angaben notwendig, die Sie über Ihren Provider bekommen. Wählen Sie in diesem Fall den Eintrag „Neuen POP3-Server anlegen“ und klicken Sie den Schalter „Weiter“.

Soll ein bestehender POP3-Server bearbeitet werden, so ist der Eintrag „bestehenden POP3-Server bearbeiten“ zu wählen. Auch hier bestätigen Sie Ihre Angabe mit den Schalter „Weiter“. Lesen Sie in diesem Fall im Kapitel 7.4.1.5 weiter.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
POP3-Server bearbeiten
Neuen POP3-Server anlegen
bestehenden POP3-Server bearbeiten
Legen Sie bitte einen neuen POP3-Server im Internet an um von diesem Mail abzuholen oder wählen Sie "bestehenden POP3-Server bearbeiten" wenn dieser bereits angelegt ist. Sie können anschließend die einzelnen Konten des POP-Servers bearbeiten.
Hinweis: Sollten Sie die lokalen Domains in der vorhergehenden Maske verändert haben, so empfiehlt es sich alle bereits angelegten POP-Server zu bearbeiten, sofern diese über POP3-Sammelpostfächer (multi-drop) verfügen.
< Zurück
Weiter >
Abbrechen

7.4.1.4. Neuen POP3-Server anlegen

Tragen Sie im freien Feld „Name des POP3-Servers“ bitte den Hostnamen oder die entsprechende IP-Adresse des Servers ein. Wie bereits erwähnt erhalten Sie die Angaben für diesen Eintrag von Ihrem Provider.

Bestätigen Sie Ihre Angabe mit dem Schalter „Weiter“. Sie gelangen nun zu den Postfächern dieses POP3-Servers. Lesen Sie bitte weiter in Kapitel 7.4.1.6

7.4.1.5. Bestehenden POP3-Server bearbeiten

Nach Anwahl dieses Menüpunktes erhalten Sie eine Auswahlmaske mit den bereits konfigurierten POP3-Servern. Wählen Sie den zu bearbeitenden Server durch Selektion aus und wählen Sie den Schalter „Weiter“. Sie gelangen daraufhin in die Bearbeitungsmaske der Postfächer wie nachfolgend beschrieben.

7.4.1.6. Postfächer bearbeiten

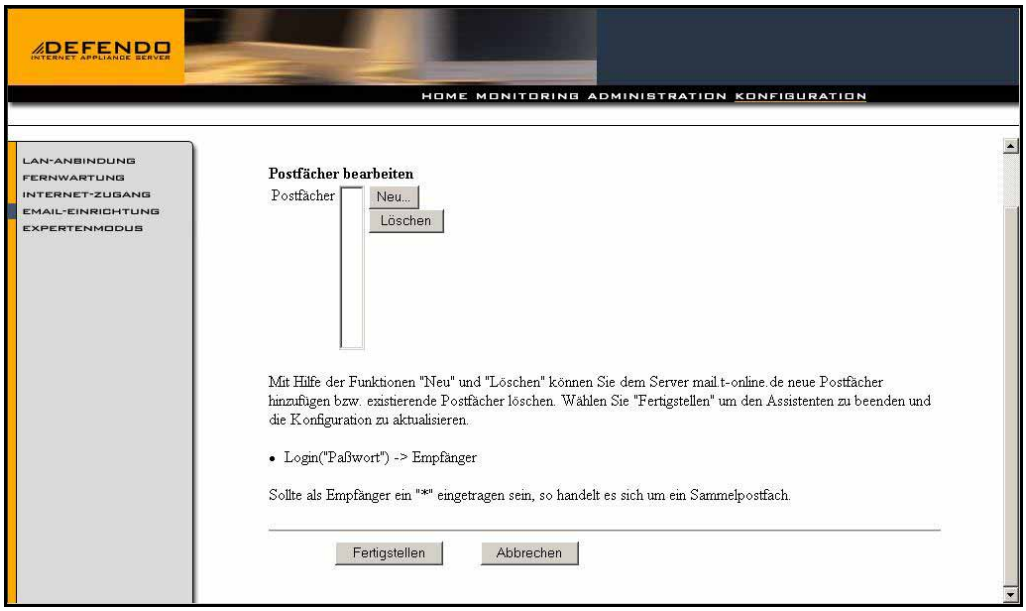
Mit Hilfe der Funktionsschalter „Neu“ und „Löschen“ können Sie dem POP3-Server neue Postfächer hinzufügen bzw. existierende Postfächer löschen.

Bereits angelegte Konten werden mit Ihrem Kontonamen (Login), dem zugehörigen Paßwort und dem lokalen Empfänger angezeigt:

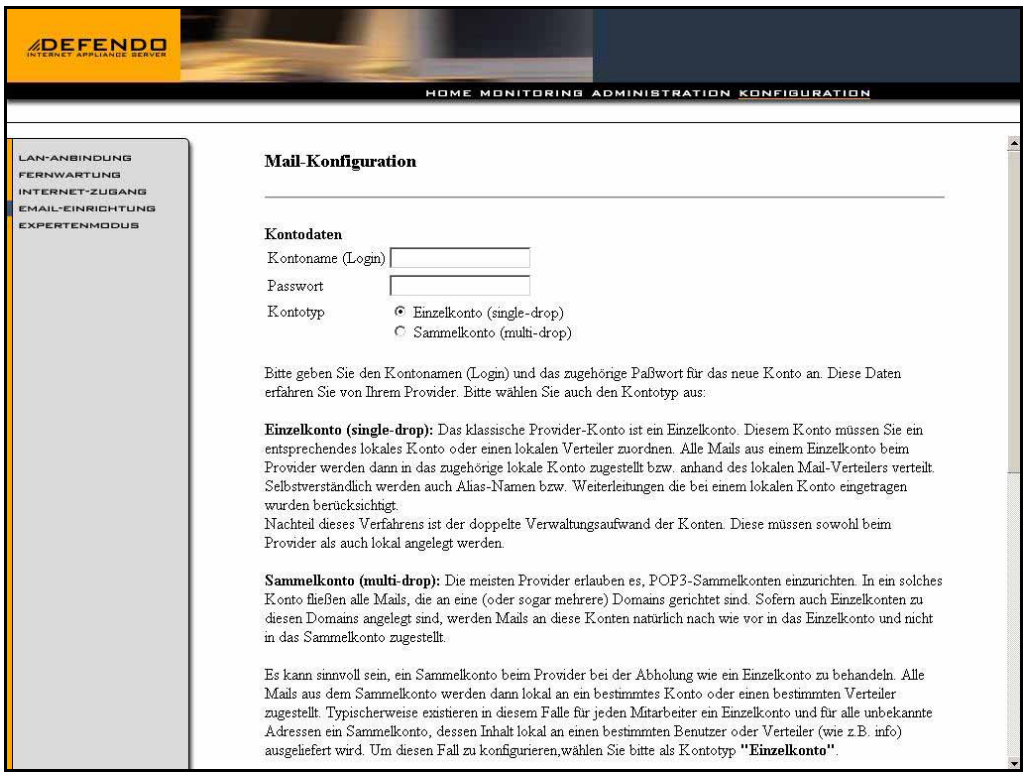
- **Login(„Paßwort“) -> Empfänger**

Sollte als Empfänger ein „*“ eingetragen sein, so handelt es sich um ein Sammelpostfach.

Wählen Sie den Schalter „Neu“ um nun ein neues Postfach anzulegen.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Postfächer bearbeiten
Postfächer
Neu...
Löschen
Mit Hilfe der Funktionen "Neu" und "Löschen" können Sie dem Server mail.t-online.de neue Postfächer hinzufügen bzw. existierende Postfächer löschen. Wählen Sie "Fertigstellen" um den Assistenten zu beenden und die Konfiguration zu aktualisieren.
• Login("Paßwort") -> Empfänger
Sollte als Empfänger ein "*" eingetragen sein, so handelt es sich um ein Sammelpostfach.
Fertigstellen
Abbrechen

7.4.1.7. Hinzufügen eines Postfaches


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Kontodaten
Kontoname (Login)
Passwort
Kontotyp
Einzelkonto (single-drop)
Sammelkonto (multi-drop)
Bitte geben Sie den Kontonamen (Login) und das zugehörige Paßwort für das neue Konto an. Diese Daten erfahren Sie von Ihrem Provider. Bitte wählen Sie auch den Kontotyp aus:
Einzelkonto (single-drop): Das klassische Provider-Konto ist ein Einzelkonto. Diesem Konto müssen Sie ein entsprechendes lokales Konto oder einen lokalen Verteiler zuordnen. Alle Mails aus einem Einzelkonto beim Provider werden dann in das zugehörige lokale Konto zugestellt bzw. anhand des lokalen Mail-Verteilers verteilt. Selbstverständlich werden auch Alias-Namen bzw. Weiterleitungen die bei einem lokalen Konto eingetragen wurden berücksichtigt.
Nachteil dieses Verfahrens ist der doppelte Verwaltungsaufwand der Konten. Diese müssen sowohl beim Provider als auch lokal angelegt werden.
Sammelkonto (multi-drop): Die meisten Provider erlauben es, POP3-Sammelkonten einzurichten. In ein solches Konto fließen alle Mails, die an eine (oder sogar mehrere) Domains gerichtet sind. Sofern auch Einzelkonten zu diesen Domains angelegt sind, werden Mails an diese Konten natürlich nach wie vor in das Einzelkonto und nicht in das Sammelkonto zugestellt.
Es kann sinnvoll sein, ein Sammelkonto beim Provider bei der Abholung wie ein Einzelkonto zu behandeln. Alle Mails aus dem Sammelkonto werden dann lokal an ein bestimmtes Konto oder einen bestimmten Verteiler zugestellt. Typischerweise existieren in diesem Falle für jeden Mitarbeiter ein Einzelkonto und für alle unbekannte Adressen ein Sammelkonto, dessen Inhalt lokal an einen bestimmten Benutzer oder Verteiler (wie z.B. info) ausgeliefert wird. Um diesen Fall zu konfigurieren,wählen Sie bitte als Kontotyp "Einzelkonto".

Bitte geben Sie den Kontonamen (Login) und das zugehörige Paßwort für das neue Konto an. Diese Daten erfahren Sie von Ihrem Provider. Bitte wählen Sie auch den Kontotyp aus.

Einzelkonto (single-drop):

Das klassische Provider-Konto ist ein Einzelkonto. Diesem Konto müssen Sie ein entsprechendes lokales Konto oder einen lokalen Verteiler zuordnen. Alle Mails aus einem Einzelkonto beim Provider werden dann in das zugehörige lokale Konto zugestellt bzw. anhand des lokalen Mail-Verteilers verteilt. Selbstverständlich werden auch Alias-Namen bzw. Weiterleitungen die bei einem lokalen Konto eingetragen wurden berücksichtigt. Nachteil dieses Verfahrens ist der doppelte Verwaltungsaufwand der Konten. Diese müssen sowohl beim Provider als auch lokal auf dem DEFENDO angelegt werden.

Sammelkonto (multi-drop):

Die meisten Provider unterstützen es, POP3-Sammelkonten einzurichten. In ein solches Konto fließen alle Mails, die an eine (oder sogar

mehrere) Domains gerichtet sind. Sofern auch Einzelkonten zu diesen Domains angelegt sind, werden die Mails natürlich nach wie vor in das Einzelkonto und nicht in das Sammelkonto zugestellt.

Es kann sinnvoll sein, ein Sammelkonto beim Provider bei der Abholung wie ein Einzelkonto zu behandeln. Alle Mails aus dem Sammelkonto werden dann lokal an ein bestimmtes Konto oder einen bestimmten Verteiler zugestellt. Typischerweise existieren in diesem Falle für jeden Mitarbeiter ein Einzelkonto und für alle unbekannte Adressen ein Sammelkonto, dessen Inhalt lokal an einen bestimmten Benutzer oder Verteiler (wie z.B. info) ausgeliefert wird. Um diesen Fall zu konfigurieren, wählen Sie bitte als lokalen Kontotyp „Einzelkonto“.

Wird ein Sammelkonto beim Provider auch lokal als Sammelkonto behandelt, so wird beim Abholen der Mail aus dem Provider-Konto versucht, den ursprünglichen Empfänger zu rekonstruieren. Ist dies möglich, so wird die Mail lokal an diesen Empfänger zugestellt. Um ein neues Mail-Konto oder einen neuen Verteiler anzulegen ist auf Seiten des Providers kein Eingriff notwendig - die Kontenverwaltung wird ausschließlich lokal vorgenommen. Wenn Sie dieses Verhalten wünschen, wählen Sie bitte den Kontotyp „Sammelkonto“.

Hinweis:

Nicht immer lässt sich der eigentliche Empfänger bei einer Mail aus einem Sammelkonto rekonstruieren! Problematisch sind insbesondere folgende Fälle:

- *Bestimmte Provider-Mail-Server, die die benötigte Information nicht in den Mails hinterlegen.*
- *Mails die anhand von Verteilerlisten oder Weiterleitungen an mehrere Benutzer verteilt werden und vom gleichen Provider-Mail-Server verwaltet werden (insbesondere bei Mailling-Listen relevant).*
- *Mails die als blinde Kopie (Bcc) verschickt wurden.*

Sollten sich in diesem Zusammenhang Probleme ergeben, so sollte man eine Mischlösung aus Einzel- und Sammelkonten wählen: Neu eingerichtet Adressen können dann mit Hilfe des Sammelkontos sofort in Betrieb genommen werden. Ergeben sich wiederholte Fehlzustellungen, so wird das Konto zu einem späteren Zeitpunkt beim Provider als Einzelkonto angelegt.

zusätzlicher Hinweis:

Lässt sich der Empfänger einer Mail aus einem Sammelkonto nicht rekonstruieren, so wird diese Mail stets an den Administrator zugestellt.

Sollten Sie bei Ihrem Provider über ein Einzelkonto verfügen, wählen Sie bitte als „lokaler Kontotyp“ das Einzelkonto. Bei einem Sammelkonto ist der entsprechende Eintrag zu wählen. Lesen Sie zu Sammelkonten im Kapitel 7.4.1.9 weiter. Alle Eingaben werden über den Schalter „Weiter“ am Ende dieser Seite bestätigt und in die entsprechende Maske gewechselt.

7.4.1.8. Postfächer über Einzelkonto

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
lokaler Empfänger
Mails aus diesem Postfach zustellen an mustereinzel
Bitte geben Sie den Namen des Kontos oder des Mail-Verteilers an, an den Mail aus dem Provider-Postfach mustereinzel zugestellt werden soll.
Achtung: Bitte geben Sie hier keine vollständige Mail-Adresse sondern lediglich den Konto- oder Verteiler-Namen ohne Domain an.
< Zurück
Weiter >
Abbrechen

Tragen Sie im Feld „lokaler Empfänger“ bitte den Namen des Kontos oder des Mail-Verteilers ein, an den Mails aus dem Provider-Postfach zugestellt werden sollen.

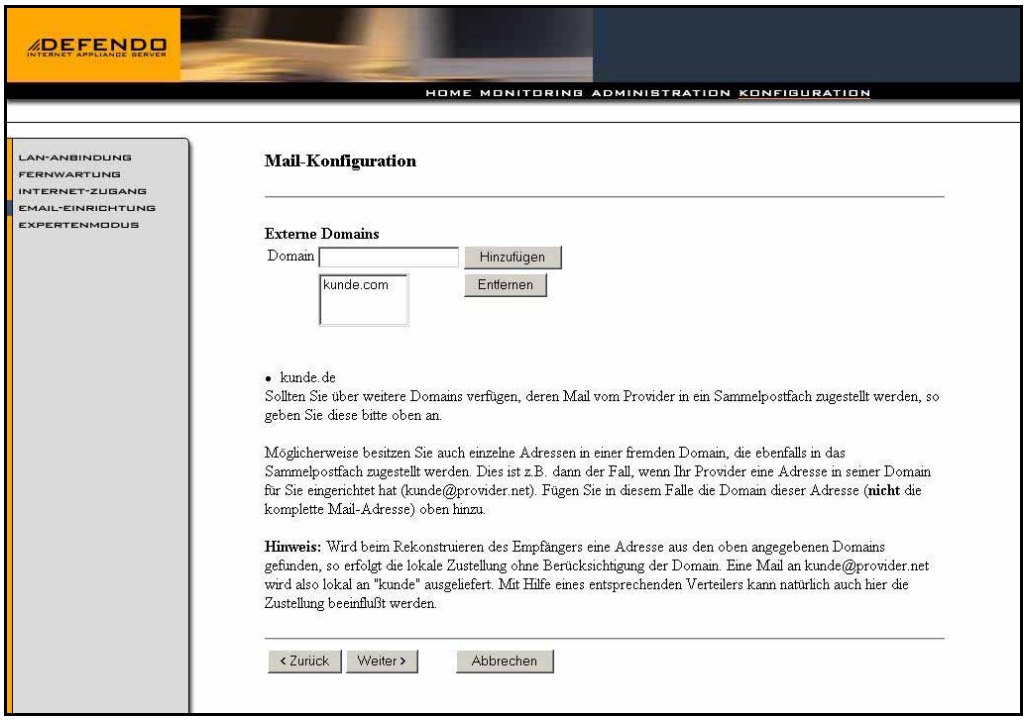
> *Hinweis:*
>
> *Bitte geben Sie hier keine vollständige eMail-Adresse sondern lediglich den Konto- oder Verteiler-Namen ohne Domain an.*

Nachdem diese Angaben gemacht wurden und über den Schalter „Weiter“ bestätigt sind, gelangen Sie wieder in die Maske „Postfächer bearbeiten“ (siehe Kapitel 7.4.1.6). Hier können nun weitere Postfächer bearbeitet werden, oder die Eingaben gespeichert und die entsprechenden Dienste gestartet werden. Dies geschieht über den Schalter „Fertigstellen“ am Ende der Seite. Die Bestätigung über die erfolgreiche Konfiguration wird Ihnen über eine Maske angezeigt.

7.4.1.9. Postfächer über Sammelkonto

Um den ursprünglichen Empfänger einer Mail aus einem Sammelpostfach zu rekonstruieren, wird die Mail nach Adressen durchsucht, die zu einer der lokalen Domains gehören.

Sollten Sie über weitere Domains verfügen, deren Mails vom Provider in Ihr Sammelpostfach zugestellt werden, so geben Sie diese bitte an. Tragen Sie diese Domain in das Feld „Domain“ ein und bestätigen Sie Ihre Angabe über den Schalter „Hinzufügen“. Wollen Sie etwaige Eintragungen löschen, so selektieren Sie diese und klicken Sie auf den Schalter „Entfernen“.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Externe Domains
Domain
Hinzufügen
kunde.com
Entfernen
• kunde.de
Sollten Sie über weitere Domains verfügen, deren Mail vom Provider in ein Sammelpostfach zugestellt werden, so geben Sie diese bitte oben an.
Möglicherweise besitzen Sie auch einzelne Adressen in einer fremden Domain, die ebenfalls in das Sammelpostfach zugestellt werden. Dies ist z.B. dann der Fall, wenn Ihr Provider eine Adresse in seiner Domain für Sie eingerichtet hat (kunde@provider.net). Fügen Sie in diesem Falle die Domain dieser Adresse (nicht die komplette Mail-Adresse) oben hinzu.
Hinweis: Wird beim Rekonstruieren des Empfängers eine Adresse aus den oben angegebenen Domains gefunden, so erfolgt die lokale Zustellung ohne Berücksichtigung der Domain. Eine Mail an kunde@provider.net wird also lokal an "kunde" ausgeliefert. Mit Hilfe eines entsprechenden Verteilers kann natürlich auch hier die Zustellung beeinflußt werden.
< Zurück
Weiter >
Abbrechen

Möglicherweise besitzen Sie auch einzelne Adressen in einer fremden Domain, die ebenfalls in das Sammelpostfach zugestellt werden. Dies ist z.B. dann der Fall, wenn Ihr Provider eine Adresse in seiner Domain für Sie eingerichtet hat (kunde@provider.net). Fügen Sie in diesem Falle die Domain dieser Adresse (**nicht** die komplette Mail-Adresse) oben hinzu.

Hinweis:

Wird beim Rekonstruieren des Empfängers eine Adresse aus den oben angegebenen Domains gefunden, so erfolgt die lokale Zustellung ohne Berücksichtigung der Domain. Eine Mail an kunde@provider.net wird also lokal an „kunde“ ausgeliefert. Mit Hilfe eines entsprechenden Verteilers kann natürlich auch hier die Zustellung beeinflußt werden.

Nach der Bestätigung über den Schalter „Weiter“ am Ende dieser Seite haben Sie die Möglichkeit weitere Postfächer anzulegen oder zu löschen.

DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Postfächer bearbeiten
Postfächer
mustereinzel("test") -> mustereinzel
mustersammel("test") -> *
Neu...
Löschen
Mit Hilfe der Funktionen "Neu" und "Löschen" können Sie dem Server mail.provider.de neue Postfächer hinzufügen bzw. existierende Postfächer löschen. Wählen Sie "Fertigstellen" um den Assistenten zu beenden und die Konfiguration zu aktualisieren.
• Login("Paßwort") -> Empfänger
Sollte als Empfänger ein "*" eingetragen sein, so handelt es sich um ein Sammelpostfach.

Mit Hilfe der Funktionsschalter „Neu“ und „Löschen“ können Sie dem POP3-Server neue Postfächer hinzufügen bzw. existierende Postfächer löschen.

Bereits angelegte Konten werden mit Ihrem Kontonamen (Login), dem zugehörigen Paßwort und dem lokalen Empfänger angezeigt:

- Login(„Paßwort“) -> Empfänger

Sollte als Empfänger ein „*“ eingetragen sein, so handelt es sich um ein Sammelpostfach.

Sind alle Angaben zu Ihren existierenden Postfächern abgeschlossen, wählen Sie bitte den Schalter „Fertigstellen“ am Ende dieser Seite. Ihnen wird die Ausführung der Konfiguration sowie der Start der entsprechenden Dienste angezeigt.

7.4.2. DEFENDO stellt Mails an einen anderen Mail-Server im LAN zu

In diesem Falle werden die Mails zwar vom Provider abgeholt, aber dann gleich an einen bestehenden anderen Mail-Server im LAN weitergeleitet.

Dies ist z. B. dann interessant, wenn Sie bereits einen Microsoft Exchange, Lotus Notes- oder einen Tobit David-Server im Einsatz haben.

Wählen Sie den Menüpunkt „DEFENDO holt Mail ab und stellt sie an einen anderen Mail-Server im LAN zu“ in der Eingangsmaske des Konfigurations-Assistenten „eMail Einrichtung“ und bewegen Sie sich mit Hilfe des Schalter „Weiter“ in die nächste Konfigurationsmaske.

7.4.2.1. Angabe des internen Mail-Servers

Sie gelangen nun in die Abfragemaske für die Angaben des internen Mail-Servers. Geben Sie bitte die IP-Adresse oder den DNS-Namen des Mail-Servers an, an den der DEFENDO die Mails mit SMTP zustellen soll.

Hinweis:

Wenn Sie einen DNS-Namen eintragen, so prüfen Sie bitte ob dieser auch vom DEFENDO korrekt in eine IP-Adresse aufgelöst werden kann.

DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Vom Mail-Server 192.168.0.3 verwaltete Domains
Domain
Hinzufügen
kunde.de
Entfernen
Tragen Sie hier alle Domains ein, die vom Mail-Server 192.168.0.3 verwaltet werden. Alle Mails, die an eine dieser Domains gerichtet sind, werden nicht in das Internet weitergeleitet sondern auf Viren geprüft und anschließend an den Mail-Server 192.168.0.3 mit SMTP zugestellt. Richten Sie dazu bitte entsprechende Mail-Verteiler und Benutzer-Konten auf 192.168.0.3 ein.
Achtung: Um Mail-Schleifen zu vermeiden, muß der Mail-Server 192.168.0.3 die oben aufgeführten Domains als lokale Domains erkennen. Er darf seinerseits nicht versuchen, diese Mails in das Internet zu versenden.
Weiter >
Abbrechen

Bestätigen Sie die Angabe des internen Mail-Server mit dem Schalter „Weiter“. Sie erhalten nun die Maske der verwalteten Domains.

7.4.2.2. Die Domains des internen Mail-Servers

Tragen Sie hier alle Domains ein, die vom Ihrem internen Mail-Server verwaltet werden. Alle Mails, die an eine dieser Domains gerichtet sind, werden **nicht** in das Internet weitergeleitet sondern umgehend an den internen Mail-Server mit SMTP zugestellt. Richten Sie dazu bitte entsprechende Mail-Verteiler und Benutzer-Konten auf Ihrem internen Mail-Server ein.

Hinweis:

Um Mail-Schleifen zu vermeiden, muß der interne Mail-Server die oben aufgeführten Domains als lokale Domains erkennen. Er darf seinerseits nicht versuchen, diese eMails in das Internet zu versenden.

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Interner Mail-Server
Interner Mail-Server 192.168.0.3
Geben Sie bitte die IP-Adresse oder den DNS-Namen des Mail-Servers an, an den Defendo die Mails mit SMTP weitergeleitet werden sollen.
Hinweis: Wenn Sie einen DNS-Namen eintragen, so prüfen Sie bitte ob dieser auch vom Defendo korrekt in eine IP-Adresse aufgelöst werden kann.
Weiter >
Abbrechen

Über den Schalter „Weiter“ werden Ihre Angaben zur Vervollständigung der Konfiguration verwendet. Der DEFENDO wechselt nun in die nächste Konfigurationsmaske. Diese Masken sind identisch mit der Option „DEFENDO holt Mail ab und ist selbst Mail-Server für Ihr LAN“. Bitte lesen Sie die Beschreibung der nachfolgenden Masken unter dem Kapitel 7.4.1 nach.

7.4.3. Weitere Optionen unter eMail-Einrichtung

7.4.3.1. POP3-Server mit allen Postfächern löschen

Mit Hilfe dieser Funktion können ganze bestehende POP3-Server auf dem DEFENDO gelöscht werden. Nach der Bestätigung des Schalter „Weiter“ gelangen Sie in die Auswahlmaske der bestehenden POP3-Server auf Ihrem DEFENDO . Selektieren Sie den zu löschen Server (Mehrfachselektionen sind möglich) und klicken Sie auf den Schalter

„Fertigstellen“. Bevor jedoch gelöscht wird, muss eine entsprechende Sicherheitsabfrage bestätigt werden.

In einer weiteren Maske wird Ihnen der Löschvorgang bestätigt.

7.4.3.2. Zustellungs- und Abholzeiten für Mails

Damit der DEFENDO weiß, wann er etwaige eMails versenden bzw. abholen soll, ist die Konfiguration dieser Einstellungen notwendig.

Zuerst wird Ihnen eine Eingabemaske angezeigt, in der die Konfiguration der Verbindung zum Provider abgefragt wird. Der DEFENDO kann bei PPP-Wählverbindungen in das Internet die Mail-Kommunikation mit dem Aufbau der Wählverbindung koppeln. Wählen Sie in diesem Falle bitte „Wählleitung“ aus. Wählen Sie bitte „Standleitung“ wenn einer der folgenden Punkte auf Sie zutrifft:

- Der DEFENDO ist über eine Standleitung an das Internet angebunden
- Der DEFENDO ist über eine Wählleitung mit Flat-Rate an das Internet angebunden und dabei so konfiguriert, daß die Verbindung praktisch nie getrennt wird. Wenn es sich also quasi um eine Standleitung handelt.
- Der DEFENDO ist über einen externen Router mit Wählleitung an das Internet angebunden
- Die Wählverbindung in das Internet wird nicht über das PPP-Protokoll abgewickelt (Der Name Ihrer Internet-Schnittstelle beginnt in diesem Falle weder mit ippp noch mit adsl, siehe hierzu Kapitel 12.1).

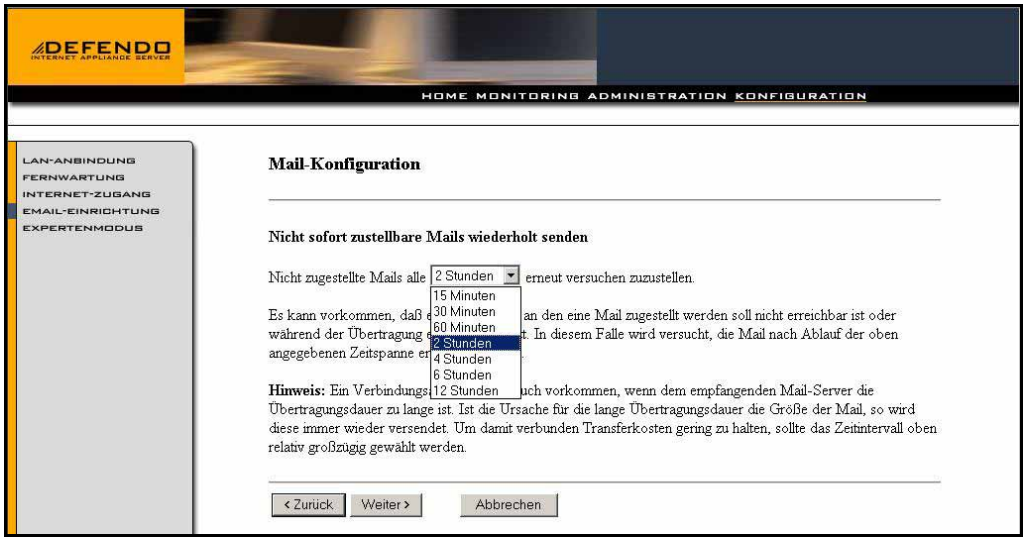
DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Stand- oder Wählleitung?
Wählleitung
Standleitung
Der Defendo kann bei PPP-Wählverbindungen in das Internet die Mail-Kommunikation mit dem Aufbau der Wählverbindung koppeln. Wählen Sie in diesem Falle bitte "Wählleitung" aus.
Wählen Sie bitte "Standleitung" wenn einer der folgenden Punkte auf Sie zutrifft:
• Der Defendo ist über eine Standleitung an das Internet angebunden
• Der Defendo ist über einen externen Router mit Wählleitung an das Internet angebunden
• Die Wählverbindung in das Internet wird nicht über das PPP-Protokoll abgewickelt (Der Name Ihrer Internet-Schnittstelle beginnt in diesem Falle weder mit ippp noch mit adsl)..
Weiter >
Abbrechen

7.4.3.2.1. Versenden von Mails über Standleitung

Bei einer Verbindung über eine Standleitung haben Sie zusätzlich die Einstellungsmöglichkeit, nicht zugestellte Mails (in bestimmten Zeitabschnitten) einen erneuten Versuch der Zustellung zu unterwerfen, da es vorkommen kann, dass ein Mail-Server, an den eine Mail zugestellt werden soll nicht erreichbar ist, oder während der Übertragung ein Fehler auftritt. In diesem Falle wird versucht, die Mail nach Ablauf der oben angegebenen Zeitspanne erneut zuzustellen.

Hinweis:

Ein Verbindungsabbruch kann auch vorkommen, wenn dem empfangenden Mail-Server die Übertragungsdauer zu lange dauert. Ist die Ursache für die lange Übertragungsdauer die Größe der Mail, so wird diese immer wieder versendet. Um damit verbundene Transferkosten gering zu halten, sollte das Zeitintervall oben relativ großzügig gewählt werden.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Nicht sofort zustellbare Mails wiederholt senden
Nicht zugestellte Mails alle 2 Stunden erneut versuchen zuzustellen.
15 Minuten
30 Minuten
60 Minuten
2 Stunden
4 Stunden
6 Stunden
12 Stunden
Es kann vorkommen, daß
an den eine Mail zugestellt werden soll nicht erreichbar ist oder
während der Übertragung
. In diesem Falle wird versucht, die Mail nach Ablauf der oben
angegebenen Zeitspanne er
Hinweis: Ein Verbindungs
uch vorkommen, wenn dem empfangenden Mail-Server die
Übertragungsdauer zu lange ist. Ist die Ursache für die lange Übertragungsdauer die Größe der Mail, so wird
diese immer wieder versendet. Um damit verbunden Transferkosten gering zu halten, sollte das Zeitintervall oben
relativ großzügig gewählt werden.
< Zurück
Weiter >
Abbrechen

Wählen Sie bitte Ihren gewünschten Zeitintervall aus, indem der DEFENDO nicht zugestellte Mails erneut versenden soll. Über den Schalter „Weiter“ wird Ihre Angabe übernommen.

Lesen Sie bitte im Kapitel 7.4.3.2.3 weiter.

7.4.3.2.2. Versenden von Mails über Wählleitung

Nach der Bestätigung des Menüpunktes „Wähleitung“ im Optionsmenü über den Schalter „Weiter“ wird abgefragt, ob Ihre Mails sofort versendet, oder ob diese gesammelt werden sollen.

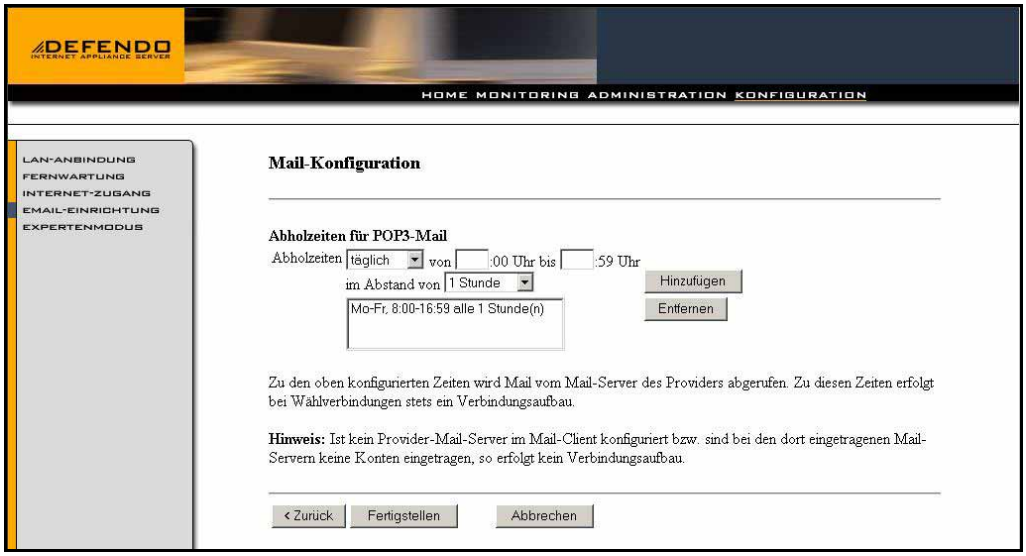
Wählen Sie „sammeln“ um Verbindungskosten zu sparen. Ausgehende Mails werden erst beim nächsten Verbindungsaufbau in das Internet versendet. Ein Verbindungsaufbau wird ausgelöst wenn beispielsweise ein Benutzer surft oder eine Mailabholung gemäß Zeitplan ausgeführt wird.

DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Ausgehende Mails sammeln oder sofort versenden?
sofort versenden
sammeln
Wählen Sie "sammeln" um Verbindungskosten zu sparen. Ausgehende Mails werden erst beim nächsten Verbindungsaufbau in das Internet versendet. Ein Verbindungsaufbau wird ausgelöst wenn beispielsweise ein Benutzer surft oder eine Mailabholung gemäß Zeitplan ausgeführt wird.
< Zurück
Weiter >
Abbrechen

Bestätigen Sie Ihre Angaben mit Hilfe des Schalter „Weiter“. Sie gelangen nun in die Abfragemaske der Abholzeiten.

7.4.3.2.3. Abholzeiten für POP3-Mails

Für beide Verbindungsarten ist die Angabe der Abholzeiten notwendig. Hierbei ist es möglich, nur zu Ihren Arbeitszeiten eMails abzuholen. So können teure Verbindungsaufbauten vermieden werden, wenn Mails nachts oder am Wochenende ohnehin nicht von ihrem Empfänger gelesen werden.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
LAN-ANBINDUNG
FERNWARTUNG
INTERNET-ZUGANG
EMAIL-EINRICHTUNG
EXPERTENMODUS
Mail-Konfiguration
Abholzeiten für POP3-Mail
Abholzeiten täglich von :00 Uhr bis :59 Uhr
im Abstand von 1 Stunde
Hinzufügen
Entfernen
Mo-Fr, 8:00-16:59 alle 1 Stunde(n)
Zu den oben konfigurierten Zeiten wird Mail vom Mail-Server des Providers abgerufen. Zu diesen Zeiten erfolgt bei Wählverbindungen stets ein Verbindungsaufbau.
Hinweis: Ist kein Provider-Mail-Server im Mail-Client konfiguriert bzw. sind bei den dort eingetragenen Mail-Servern keine Konten eingetragen, so erfolgt kein Verbindungsaufbau.
< Zurück
Fertigstellen
Abbrechen

Tragen Sie in die entsprechenden Felder die gewünschten Tage sowie Start- und Stopuhrzeit für die Mailabholung ein. Zudem ist die Angabe der Wartezeit zwischen den Abholversuchen anzugeben.

Zu den oben konfigurierten Zeiten werden Mails vom Mail-Server des Providers abgerufen. Zu diesen Zeiten erfolgt bei Wählverbindungen stets ein Verbindungsaufbau.

> *Hinweis:*
>
> *Ist kein Provider-Mail-Server konfiguriert bzw. sind bei den eingetragenen Mail-Servern keine Konten eingetragen, so erfolgt kein Verbindungsaufbau (siehe Kapitel 12.7).*

Nachdem Sie alle Angaben erledigt haben und diese über den Schalter „Fertigstellen“ bestätigt haben, erhalten Sie eine Bestätigung über die Konfiguration der eMail-Einstellungen.

8. Einstellungen der LAN-PCs fürs Internet

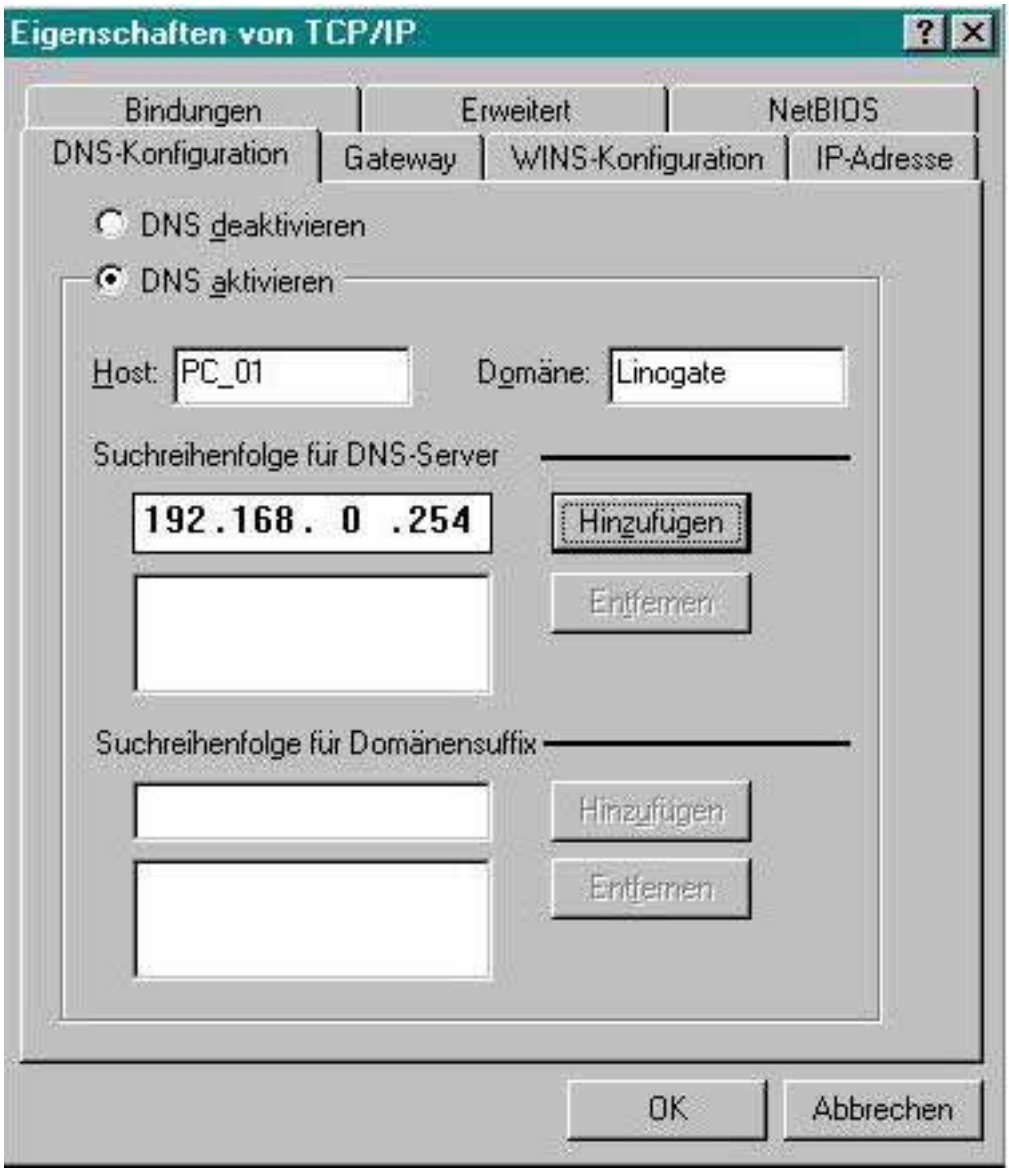
Damit Ihre PCs in Ihrem LAN nun auch den Zugang zum Internet über den DEFENDO nützen können, sind Einstellungen an ihnen vorzunehmen.

8.1. Verwendung eines DHCP-Servers

Sollten Sie in Ihrem LAN einen DHCP-Server verwenden, so sind diese Einstellungen nur am DHCP-Server notwendig. Es reicht dann aus, die Workstations neu zu booten. Fügen Sie für den Eintrag „Gateway“ die IP-Adresse des DEFENDO ein. Sollten Sie Windows NT 4.0 Server mit DHCP-Server verwenden, ist dieser als „Router“ deklariert. Fügen Sie ebenfalls einen „DNS-Server“ Eintrag hinzu. Auch hier ist die IP-Adresse des DEFENDO einzutragen. Somit sind die Einstellungen abgeschlossen.

8.2. Einstellungen am lokalen PC

Sollten Sie nicht über einen DHCP-Server im Netzwerk verfügen, so sind folgende Einträge in Ihrer Netzwerkumgebung am PC zu machen. Wechseln Sie wie im Kapitel 6.5.3 beschrieben in die Eigenschaften Ihres IP-Protokolls für Ihre Netzwerkkarte. Wählen Sie dort den Reiter „Gateway“. Tragen Sie die IP-Adresse des DEFENDO in das vorgesehene Feld ein und bestätigen Sie Ihre Eingabe mit dem Schalter „Hinzufügen“. Ihre Eingabe wird in das darunter liegende Listenfeld übernommen.



Wechseln Sie nun auf den Reiter „DNS-Konfiguration“. Setzen die Schaltbox auf „DNS aktivieren“ und tragen Sie im Feld „Host“ einen Namen ein, der nur einmal im Netzwerk existieren darf. Hierbei empfiehlt sich der Computername des PCs.

Für den Eintrag „Domäne“ verwenden Sie bitte den Eintrag, den Sie für den DEFENDO vergeben haben. Tragen Sie unter „Suchreihenfolge für DNS-Server“ die IP-Adresse des DEFENDO ein und bestätigen Sie Ihre Angaben mit den Schalter „Hinzufügen“. Ihre Angabe wird nun in das darunter liegende Listenfeld übernommen.

Mit Anwahl des Schalters „OK“ werden Ihre Änderungen übernommen und die „Eigenschaften von TCP/IP“ Maske erscheint wieder. Auch müssen Ihre Änderungen durch den Schalter „OK“ bestätigt werden.

Ihr PC wird nun einen Neustart durchführen wollen. Bitte führen Sie diesen aus.

8.3. Einrichten des Browers

Wechseln Sie nach erfolgtem Neustart des PCs in die Systemsteuerung. Dort finden Sie das Icon „Internetoptionen“, wenn auf Ihrem Gerät der MS-Internet-Browser installiert ist. Bei Verwendung eines anderen Browsers (z. B. Netscape) sind diese Einstellungen unter den Optionen des Browsers zu machen.

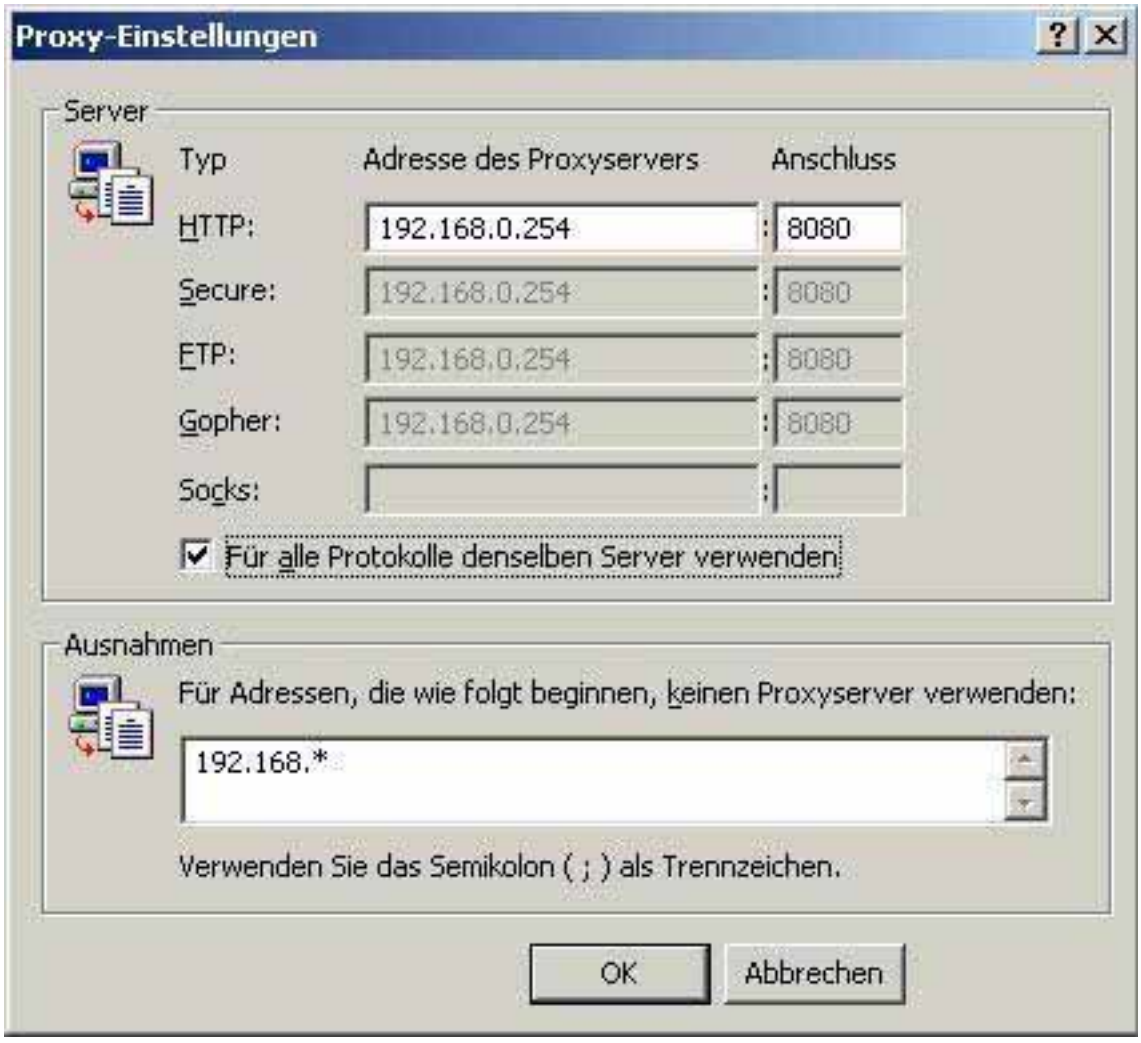
> *Hinweis:*
>
> *Sollte kein Browser installiert sein, so ist dieser unbedingt vorher zu installieren. Lesen Sie für die Vorgehensweise das Handbuch des Herstellers des zu installierenden Produktes. Verwenden Sie möglichst die aktuellste Version des Browers!*

Öffnen Sie diesen mit Hilfe des Doppelklicks der Maus und wählen dort den Reiter „Verbindungen“ an. Da die Verbindung zum Internet nun ausschließlich über das LAN und den DEFENDO aufgebaut werden kann, sollten eventuell vorhandene DFÜ-Netzwerke zur Verbindung ins Internet gelöscht werden. Wählen Sie zur Konfiguration der benötigten Einstellungen den Schalter „LAN-Einstellungen“. Sie erhalten folgende Eingabemaske:

Aktivieren Sie im Abschnitt „Proxyserver“ den Eintrag „Proxyserver verwenden“, indem Sie den Haken setzen. Es ist nun möglich, im Feld „Adresse“ und „Anschluss“ Eintragungen vorzunehmen. Tragen Sie bei „Adresse“ wiederum die IP-Adresse des DEFENDO ein. Unter „Anschluss“ verwenden Sie den Eintrag „8080“. Auf diesem Port nimmt der Proxy-Server im DEFENDO Anfragen entgegen.

Damit bei Anforderung einer IP-Adresse (die sich innerhalb Ihres LANs befindet) der Proxyserver umgangen wird, ist es notwendig den Haken beim Eintrag „Proxyserver für lokale Adressen umgehen“ zu aktivieren.

Über den Schalter „Erweitert...“ sind weitere Einstellungen möglich. Bitte wechseln Sie mit Hilfe dieses Schalters in die erweiterten Optionen.



Voreingestellt ist der Eintrag „Für alle Protokolle denselben Server verwenden“. Dieser kann so belassen werden, es sei den, Sie haben für bestimmte Dienste unterschiedliche Server im Einsatz. Bitte beachten Sie, dass bei SOCKS kein Eintrag vorgenommen werden darf.

Unter Ausnahmen empfiehlt es sich, das komplette Netz Ihres LANs anzugeben. Tragen Sie dort die Adresse Ihres LANs ein und verwenden Sie als letzte Ziffer einen „*“ (nur bei MS-I-Explorer). Hiermit ist sichergestellt, dass für eine Anforderung innerhalb Ihres LANs keine Proxyserveranfrage erfolgt. Bestätigen Sie Ihre Angaben mit dem Schalter „OK“. Ein Neustart des PCs ist hierbei nicht notwendig. Weitere spezifische und mögliche Einstellungen Ihres Browser entnehmen Sie bitte dem Handbuch des Herstellers.

Starten Sie nun Ihren Browser und versuchen Sie einen Internetzugang zu erhalten. Tragen Sie zum Beispiel im Feld Location bzw. Adresse „www.muster.de“ ein. Nach einer geringfügigen Wartezeit, die zum Auf-

bau der Verbindung sowie zum Anmelden dort benötigt wird, sollte der Browser die entsprechende Seite aufbauen. Ist dies nicht der Fall, so überprüfen Sie Ihre Einstellungen sowie wie 11.2 beschrieben, ob die entsprechenden Dienste gestartet sind.

9. Das Hauptmenü „Administration“

Unter diesem Menüpunkt können Systemeinstellungen geändert bzw. ergänzt werden. Ebenfalls finden Sie dort die Benutzerverwaltung sowie die Möglichkeit das System neu zu starten oder herunter zu fahren.

9.1. Grundeinstellungen

Hier haben Sie die Möglichkeit, den LAN-Host-Namen des DEFENDO nach Ihren Wünschen zu ändern. Auch die zugehörige LAN-Domain des DEFENDO kann entsprechend geändert werden.

> *Hinweis:*
>
> *Dieser Domainname hat nichts mit der eventuell bestehenden Windows-Domain zu tun!*

Ferner werden hier die IP-Adresse sowie die LAN-Netwerkmaske des DEFENDO eingestellt. Unter „IP-Adressen/Netzmasken der lokalen IP-Netzwerke“ können alle lokalen Netze Ihres LANs eingetragen werden, für die der DEFENDO zuständig ist. Anhand der hier eingegebenen Netzwerke unterscheidet der DEFENDO zwischen Adressen die als Intranet betrachtet werden sollen und solchen die dem Internet zuzuordnen sind. Bestimmte Dienste stehen nur den Intranet-Adressen zur Verfügung. Mit Hilfe der Schalter „Hinzufügen“ bzw. “Entfernen“ können Sie jederzeit entsprechende Einträge machen.

Wählen Sie bei „Sprache“ die Sprache aus, in der die Oberfläche dargestellt werden soll. Bitte beachten Sie, dass nach Änderung der Sprache Teile der Web-Oberfläche in der alten Sprache im internen Cache Ihres Browsers gehalten werden. Es empfiehlt sich daher, den internen Browser-Cache zu leeren bzw. Menübereiche die noch in alter Sprache dargestellt werden durch die „Aktualisieren“-Funktion Ihres Browsers explizit neu zu laden.

Bei Bestätigung des Schalters „Übernehmen“ werden die von Ihnen geänderten Eintragungen im DEFENDO gespeichert. Der Schalter „Aktuelle Werte“ liest die momentan eingestellten Werte aus dem DEFENDO aus und zeigt Sie Ihnen in dieser Maske an.

9.2. Benutzer

Hier werden die Benutzer eingerichtet bzw. geändert, die berechtigt sind, im Internet zu surfen, E-Mail-Kommunikation zu betreiben sowie weitere Berechtigungen auf Dienste des DEFENDO haben. Sie erhalten hier zunächst eine Listenbox, in der Ihre bereits angelegten Benutzer angezeigt werden. Beim ersten Start dieses Menüpunktes existiert nur ein Benutzer auf Ihrem DEFENDO , der „admin“.

9.2.1. Allgemeine Hinweise zu Benutzern

Die Rechtevergabe auf dem DEFENDO erfolgt gruppenbasierend. Es existieren vier Systemgruppen, mit denen ein Konto und damit auch ein Paßwort verknüpft ist. Mit Hilfe der Gruppenverwaltung lassen sich weitere Gruppen einrichten, mit denen jedoch kein Konto verbunden ist. Diese benutzerdefinierten Gruppen dienen ausschließlich der Erstellung von Mail-Verteilern und der strukturierten Rechte-Vergabe für den Zugriff auf das Internet über den Proxy-Cache des DEFENDO .

Ordnen Sie den Benutzer einer der folgenden Systemgruppen zu um ihm die damit verbundene Berechtigung zuzuteilen:

- **system-mail**

  Für Benutzer die dieser Gruppe zugeordnet sind wird automatisch ein E-Mail-Konto, bestehend aus dem Benutzernamen und den von Ihnen angegeben lokalen Mail-Domains auf dem DEFENDO eingerichtet (z.B. mustermann@firma.de). Alle Benutzer dieser Gruppe haben ferner Zugang zum Webmail client. Wird ein interner Mail-Server verwendet (z.B. Microsoft Ex-

change) so ist dieses Recht außer für den „admin“ ohne Belang. Der Benutzer admin kann aus der Gruppe system-mail nicht entfernt werden. Wird ein anderer Benutzer aus der Gruppe system-mail entfernt, bleibt sein Mail-Konto bestehen. Das Konto wird erst dann gelöscht, wenn der Benutzer komplett aus der Benutzerverwaltung gelöscht wird.

- **system-proxy**

  Berechtigt den Benutzer das Internet mit Hilfe eines konfigurierten Browers zu nützen. Sollte im Proxy-Cache-Server des DEFENDO die Einstellung „Zugriff nur mit Benutzeranmeldung“ aktiv sein, so wird bei einem Internetzugriff der Benutzername sowie das Passwort abgefragt. Ist die Benutzeranmeldung im Proxy-Cache deaktiviert, so ist dieses Recht ohne belang.

- **system-web**

  Berechtigt den Benutzer zum Zugriff auf die DEFENDO Administrations-Oberfläche. Wurden vom Administrator keine weiteren Berechtigungen vergeben, ist lediglich der Zugriff auf das Hauptmenü „Home“ freigegeben. Der Benutzer admin kann aus der Gruppe system-web nicht entfernt werden.

- **system-ras**

  Berechtigt den Benutzer z. B. von einem Home-Office oder einer Außenstelle via DFÜ-Netzwerk eine Einwahlverbindung mit dem DEFENDO aufzubauen, um sich dann z. B. an einer Windows-Domäne oder einen Netware-Server (wenn dieser über ein IP-Protokoll verfügt) anzumelden. Somit wäre auch ein Internetzugang von der Außenstelle über das Firmen-LAN möglich. Wenn keine entsprechende RAS-Schnittstelle auf dem DEFENDO konfiguriert ist, hat dieses Recht keine Bedeutung.

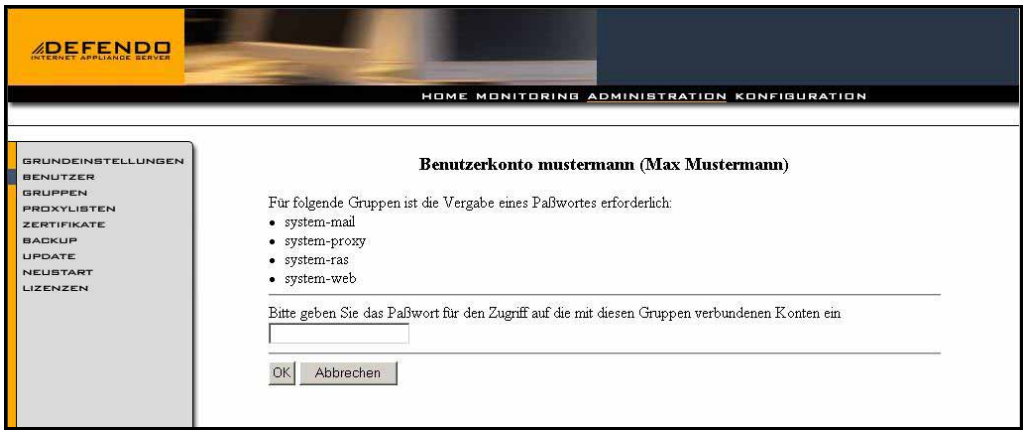
Bitte beachten Sie bei der Vergabe der Benutzernamen, dass die Verwendung von Umlauten sowie Leerzeichen nicht zugelassen wird. Es dürfen außerdem nur Kleinbuchstaben und Ziffern verwendet werden. Als Sonderzeichen sind ferner der Bindestrich (-), der Punkt (.) und der Unterstrich (_) zulässig. Der Benutzername muß mit einem Kleinbuchstaben beginnen. Eine Beschränkung der Länge besteht nicht. Eine Verwendung von folgenden Benutzernamen ist nicht möglich, da es sich hierbei um sogenannte Systemkonten handelt: *bin, daemon, ftp, games, mail, root, sync, uucp, adm, lp, shutdown, halt, news, operator gopher, nobody, admin, apache, intranet, www, squid, ftpadmin, firewall, snort*.

9.2.2. Aufnahme / Ändern von Benutzern

Tragen Sie im Feld „Benutzer Login“ den entsprechenden Namen des Benutzer ein. Empfehlenswert ist es, den Namen zu wählen, mit dem sich der Benutzer auch schon am Netzwerkbetriebssystem anmeldet. Unter vollständiger Name kann dieser ganz ausgeschrieben eingetragen werden. Dieses ist ein reines Informationsfeld. Eine Eintragung ist nicht notwendig.

Wählen Sie den Schalter „Hinzufügen“, um notwendige weitere Einstellungen zu diesem Benutzer einzutragen. Zum Ändern selektieren Sie den entsprechenden Benutzer und wählen den Schalter „Bearbeiten“.

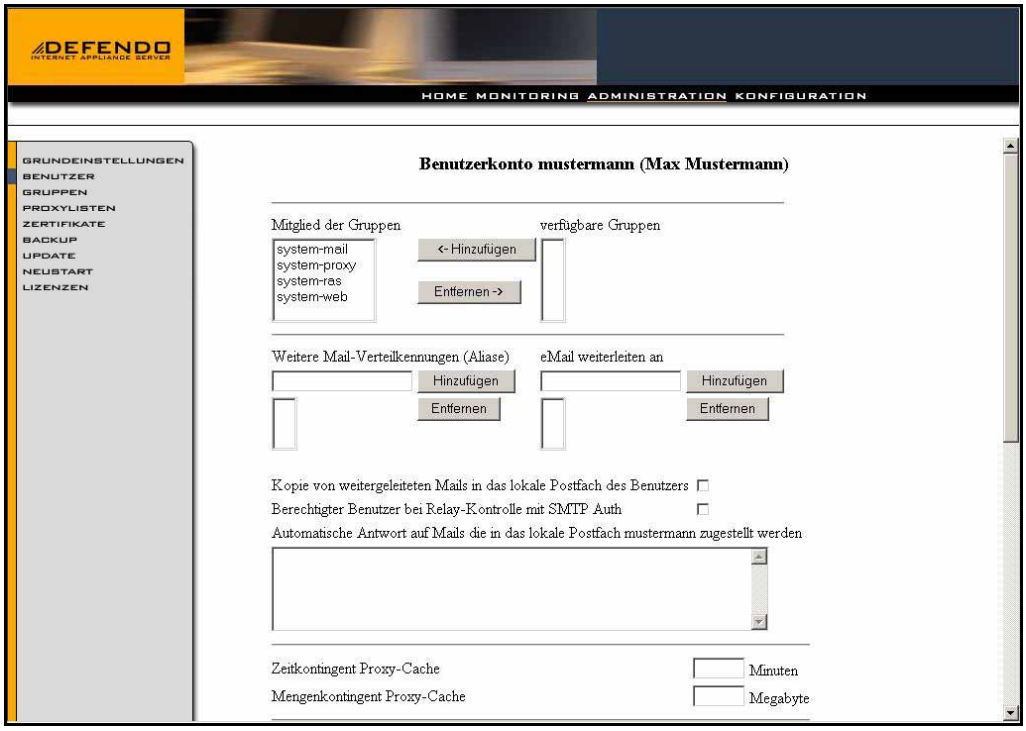
Im ersten Abschnitt der Eingabemaske sehen Sie die dem Benutzer zugeordneten bzw. die noch verfügbaren Gruppen. Bei einer Neuanlage eines Benutzers ist dieser zunächst keiner Gruppe zugeordnet. Insbesondere sind also auch noch keinerlei Konten für den Benutzer angelegt, da er dazu in entsprechende Systemgruppen aufgenommen werden muß. Um den Benutzer in Gruppen aufzunehmen, wählen Sie bitte die gewünschte Gruppe bzw. mehrere Gruppen mit Hilfe der Mehrfachauswahl im rechten Listenfeld aus und bestätigen Sie Ihre Auswahl über den Schalter „Hinzufügen“. Soll der Benutzer einer oder mehreren Systemgruppen zugeordnet werden, so erscheint zunächst eine Maske, in der das zu vergebende Passwort abgefragt wird. Bitte tragen Sie dieses in das entsprechende Feld ein und bestätigen Sie Ihre Eingabe mit den Schalter „OK“.



Wiederholen Sie diesen Vorgang ggf. für weitere Gruppen, denen Sie den Benutzer zuordnen wollen. Im linken Listenfeld werden Ihnen die bereits zugewiesenen Gruppen entsprechend angezeigt.

9.2.2.1. Einstellungen für die Gruppe system-mail

Sobald Sie einen Anwender in die Gruppe system-mail aufgenommen haben, erweitert sich die Einstellungsmaske für diesen Benutzer entsprechend. Sie finden nun einen Abschnitt, mit der Möglichkeit, beliebig viele Mail-Verteilkennungen (Aliase) sowie Mail-Weiterleitungen einzutragen. Ferner lässt sich hier eine automatische Antwort auf eingehende Mails hinterlegen und die Berechtigung für den authentifzierten Mail-Versand vergeben.



Unter einem Alias ist eine weitere Mail-Adresse zu verstehen, die zusätzlich zu der Mail-Adresse die sich aus dem Kontonamen ergibt in das entsprechende Postfach zugestellt werden soll. Dieser Alias ist unabhängig von der Domain. Geben Sie diesen Alias daher bitte stets ohne @domain an. Tragen Sie die gewünschten Aliase in das dafür vorgesehene Feld ein und bestätigen Sie diese Eingabe mit dem Schalter „Hinzufügen“. Entsprechend können über den Schalter „Entfernen“ selektierte Einträge gelöscht werden. Für etwaige Mail-Weiterleitungen gehen Sie bitte genauso wie gerade beschrieben vor. Hier ist die Angabe einer vollständigen Mail-Adresse (mit @domain) zulässig.

Sollten Mail-Weiterleitungen aktiv sein, so kann über die Option „Kopie von weitergeleiteten Mails in das lokale Postfach des Benutzers“ eine Kopie der Mail in das lokale Postfach des Benutzers erzwungen werden. Andernfalls werden die Mails vollständig weitergeleitet und das lokale Postfach erhält keine neuen Mails mehr. Die Option hat keine Auswirkung, wenn keine Mail-Weiterleitung aktiv ist.

Ist der Versand von eMails über den Mail-Server des DEFENDO in das Internet nur bestimmten Benutzerkreisen gestattet, so kann der aktuelle Benutzer mit Hilfe des Schalters „Berechtigter Benutzer bei Relay-Kontrolle mit SMTP Auth“ in diesen Benutzerkreis aufgenommen werden. Diese Option berechtigt den Benutzer sowohl für den authentifizierten Mail-Versand von den internen Netzwerken in das Internet als

auch für das authentifizierte Mail-Relay für Mails vom Internet in das Internet - je nachdem, welche dieser Übertragungswege in der Mail-Server-Konfiguration an die Bedingung der erfolgreichen Benutzeranmeldung gekoppelt wurden.

Es ist möglich auf eingehende Mails automatisch eine Antwort zu generieren um z.B. den Empfang zu bestätigen oder im Falle einer längeren Abwesenheit den Absender der Mail darüber zu benachrichtigen. Als Antwort kann eine beliebige Textnachricht gesendet werden, die in das Eingabefeld unter „automatische Antwort auf Mails die in das lokale Postfach ... zugestellt werden“ eingetragen werden kann. Ist hier kein Text hinterlegt, so wird auch keine automatische Antwort generiert.

> *Hinweis:*
>
> *Eine automatische Antwort wird für jede eMail generiert, die in das entsprechende Postfach zugestellt wird. Es werden also auch Antwortmails erzeugt, wenn die Mail über einen Verteiler (Gruppe) an das entsprechende Postfach ausgeliefert wurde. Es werden hingegen keine Antwortmails erzeugt, wenn der Benutzer eingehende Mails an eine andere Adresse weitergeleitet hat ohne sich eine Kopie in das eigene Postfach zustellen zu lassen.*

9.2.2.2. Einstellungen für die Gruppe system-proxy

Sobald Sie einen Anwender in die Gruppe system-proxy aufgenommen haben, erweitert sich die Einstellungsmaske für diesen Benutzer entsprechend sofern Ihr DEFENDO über die Option Zeit- und Mengenkontingente verfügt. Sie finden nun einen Abschnitt, mit der Möglichkeit, bei dem Benutzer eine bestimmte Minutenzahl und / oder eine bestimmte Transfermenge in Megabyte zu hinterlegen. Nach Ablauf eines dieser Kontingente wird dem Benutzer das Recht über den Proxy-Cache zu surfen entzogen. Je nach Einstellung des Proxy-Caches wird dieses Kontingent in bestimmten Zeitabständen erneuert, so daß der Benutzer dann wieder den Proxy-Cache benutzen darf. Bitte beachten Sie, daß im Proxy-Cache die Benutzeranmeldung aktiviert sein muß.

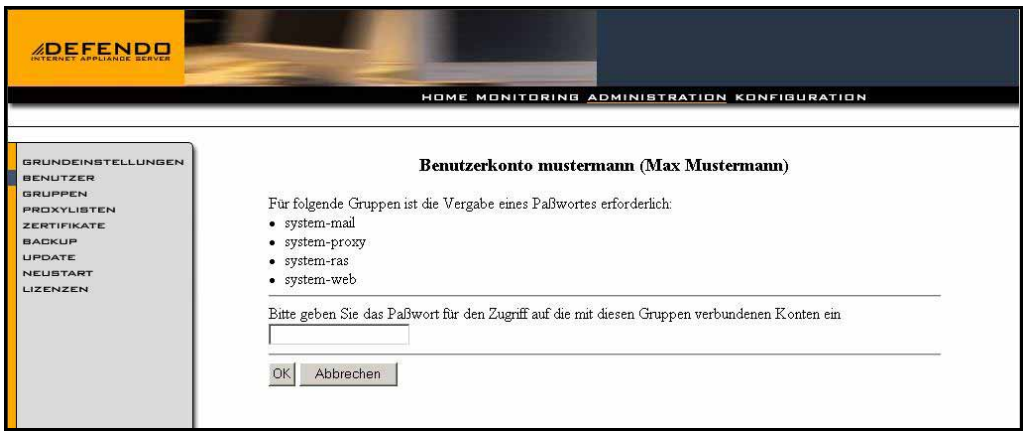
9.2.2.3. Einstellungen für die Gruppe system-web

Der Benutzer admin kann anderen Benutzern das Zugriffsrecht auf einzelne Bereiche der DEFENDO-Administrationsoberfläche erteilen. Der Benuzter muß dazu Mitglied der Gruppe system-web sein. Aktivieren Sie dazu die entsprechenden Optionshaken die den jeweiligen Menüpunkten entsprechen.

9.2.2.4. Passwortoptionen für Benutzer

Im unteren Abschnitt finden Sie die Passwortoptionen zum aktiven Benutzer. Voreingestellt ist die Möglichkeit für den Benutzer, für alle verfügbaren Dienste das Passwort selber zu ändern. Wie der Benutzer dies selbst ändern kann, ist im Kapitel 10 beschrieben. Sie können über die Auswahlhaken verhindern, dass der Benutzer selber die Passwörter der entsprechenden Dienste ändern kann. Dies kann sinnvoll sein, wenn ein Konto von verschiedenen Benutzern verwendet wird oder der Benutzer nicht über die Berechtigungen oder Kenntnisse verfügt, die Paßwörter in allen betroffenen Anwendungen (z.B. dem Mail-Client) ebenfalls anzupassen.

Über den Schalter „Passwort ändern“ können die Passwörter durch den Administrator geändert werden, wenn z.B. ein Anwender sein Paßwort vergessen hat. Für welche Dienste das Paßwort geändert werden soll kann auf der folgenden Maske ausgewählt werden. Standardmäßig wird für alle vergebenen Dienste das Passwort geändert, das Sie in der darauffolgenden Maske eintragen und bestätigen. Wollen Sie das nicht, können über die Auswahlkästchen bestimmte Dienste ausgeschlossen werden.



9.2.2.5. Benutzer löschen / Übernehmen

Soll der aktive Benutzer gelöscht werden, so kann dies über den Schalter „Benutzer löschen“ vorgenommen werden. Es werden hierbei alle Konten dieses Benutzers entfernt. Sollte ein Mail-Postfach für den Benutzer im System vorhanden sein, wird dieses gelöscht.

Zum Bestätigen Ihrer Eingaben wählen Sie den Schalter „OK“. Alle Eintragungen bzw. Änderungen werden gespeichert.

9.2.3. Hinweis zum Benutzer „admin“

Er fungiert als Systemverwalter Ihres DEFENDO. Er ist berechtigt, alle Einstellungen des Gerätes zu ändern bzw. Ergänzungen zu machen. Wichtige Systemnachrichten werden per Mail an den Benutzer admin zugestellt. Konfigurieren Sie daher bitte unbedingt eine Mail-Weiterleitung für das admin-Mailkonto, oder tragen Sie Sorge dafür, daß dieses Konto regelmäßig abgeholt wird.

9.3. Gruppen

9.3.1. Allgemeine Hinweise zu Gruppen

Die Gruppenverwaltung des DEFENDO dient dazu, Benutzer mit Berechtigungen für einzelne Dienste des DEFENDO auszustatten, Mail-Verteiler anzulegen und den Zugriff auf Internet-Seiten gruppenbasierend zu reglementieren.

Im Auslieferungszustand sind bereits die vier Systemgruppen system-mail, system-proxy, system-ras und system-web angelegt. Benutzer die diesen Gruppen zugeordnet sind, verfügen auch über ein persönliches Konto mit Paßwort, das den Zugriff auf den zu dieser Systemgruppe gehörigen Dienst ermöglicht. Diese vier Systemgruppen können nicht gelöscht werden. Die mit diesen Gruppen verknüpfte Berechtigungen können im Kapitel 9.2.1 nachgelesen werden.

Mit jeder Gruppe ist automatisch ein gleichnamiger Mail-Verteiler verknüpft. Somit ist es möglich, z.B. eine Gruppe „info“ zu erstellen. Alle Benutzer, die sich in dieser Gruppe befinden bekommen die gleiche E-Mail in ihr lokales Postfach dupliziert, die in diesem Fall an „in-

fo@ihrefirma.de“ geschickt wurde. Voraussetzung dafür ist, daß der entsprechende Benutzer auch über ein lokales Mail-Konto verfügt. Zusätzlich lassen sich zu jeder Gruppe weitere externe Mail-Empfänger angeben.

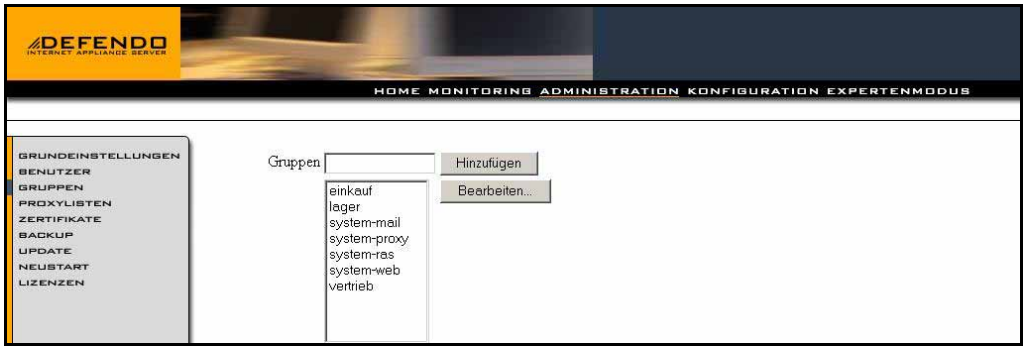
In Verbindung mit der URL-Filter-Option des Proxy-Caches lassen sich einer Gruppe beliebig viele Proxylisten zuordnen. Die Einschränkungen die sich aus den zugeordneten Proxylisten ergeben finden auf alle Gruppenmitglieder Anwendung.

Eine direkte hierarchische Organisation von Gruppen ist nicht möglich.

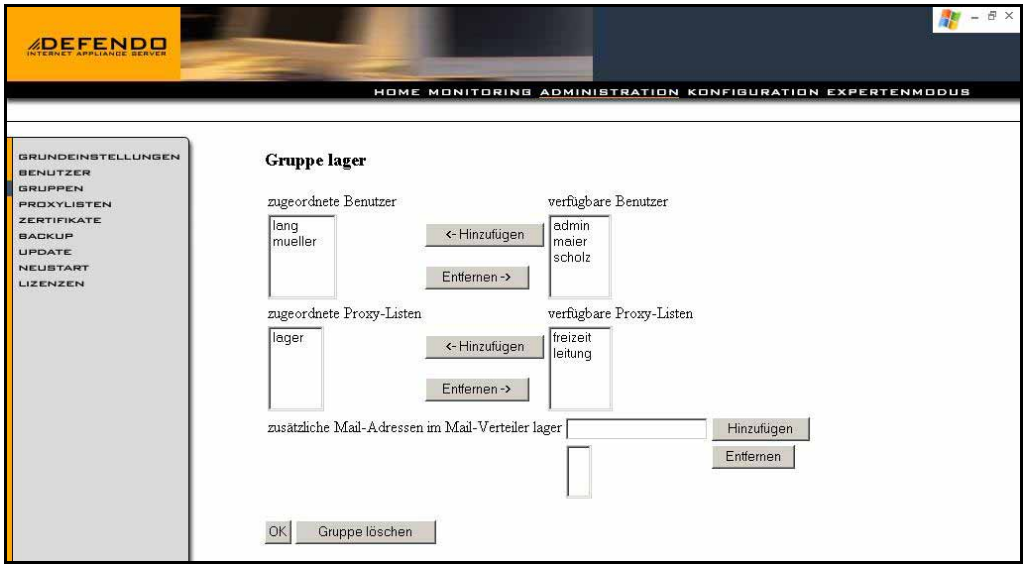
9.3.2. Aufnahme / Ändern von Gruppen

Zum Erstellen einer neuen Gruppe tragen Sie bitte in das entsprechende Feld den Namen der Gruppe ein und bestätigen Sie Ihre Eingabe mit den Schalter „Hinzufügen“. Bitte beachten Sie bei der Vergabe der Gruppennamen, dass die Verwendung von Umlauten sowie Leerzeichen nicht zugelassen wird. Es dürfen außerdem nur Kleinbuchstaben und Ziffern verwendet werden. Von Sonderzeichen sind nur der Bindestrich (-), der Punkt (.) und der Unterstrich (_) zulässig. Eine Beschränkung der Länge besteht nicht.

Wollen Sie eine bestehenden Gruppe bearbeiten, so selektieren Sie diese im Listenfeld und wählen den Schalter „Bearbeiten“.



Es wird nun in die Einstellungsmaske der entsprechenden Gruppe gewechselt.



Im oberen Bereich der Maske sehen Sie alle Benutzer, die der Gruppe bereits zugeordnet wurden sowie alle noch nicht zugeordneten Benutzer. Um Benutzer in die Gruppe aufzunehmen wählen Sie diese aus der rechten Liste aus. Mehrfachauswahl ist dabei möglich. Drücken Sie dann den Schalter „Hinzufügen“. Sofern Sie sich gerade in der Bearbeitung einer Systemgruppe befinden, erscheint danach ein Maske, in der Sie um die Eingabe eines Kennwortes für das mit dieser Systemgruppe verbunden Konto gebeten werden. Bitte geben Sie das gewünschte Paßwort ein und drücken Sie den Schalter „OK“. Bitte beachten Sie, daß im Falle einer Mehrfachauswahl von Benutzern alle neu angelegten Konten mit dem gleichen Paßwort angelegt werden.

Das Löschen von Benutzern aus der Gruppe wird entsprechend dem Hinzufügen durch Auswahl der Benutzer aus der linken Liste und dem drücken des Schalters „Entfernen“ bewerkstelligt.

Welche Proxylisten bei aktiviertem URL-Filter auf Mitglieder der aktuellen Gruppe angewendet werden sollen, können Sie mit Hilfe der folgenden Listen konfigurieren. Wählen Sie Einträge aus den verfügbaren Proxylisten und drücken Sie auf den zugehörigen Schalter „Hinzufügen“ um Listen aufzunehmen oder wählen Sie Einträge aus den zugeordneten Proxylisten und drücken Sie den Schalter „Entfernen“ wenn die gewählten Listen nicht mehr auf die Mitglieder der aktuellen Gruppe angewendet werden sollen. Eine Mehrfachauswahl bei der Auswahl von Proxylisten ist möglich. Ist die Benutzeranmeldung im Proxy-Cache deaktiviert, so werden ausschließlich die Proxylisten berücksichtigt, die der System-Gruppe system-proxy zugeordnet sind.

Achtung:

Der URL-Filter muß über die Proxy-Cache Konfiguration aktiviert werden. Andernfalls haben die Proxylisten keine Wirkung

Der DEFENDO erstellt automatisch einen Mail-Verteiler mit dem Namen der Gruppen. Alle dieser Gruppe zugeordneten Benutzer, die auch über ein lokales Mail-Konto verfügen (alle Mitglieder der Gruppe system-mail), sind automatisch in diesem Verteiler eingetragen. Wird ein Benutzer vollständig gelöscht, erhält ein Benutzer nachträglich ein lokales Mail-Konto oder wird ihm dieses entzogen, so wird dies automatisch im Mail-Verteiler berücksichtigt. Zusätzlich zu den automatisch dem Mail-Verteiler zugeordneten Benutzern lassen sich im Bereich „zusätzliche Mail-Adressen im Mail-Verteiler ...“ weitere Empfänger hinzufügen. Geben Sie hier z.B. externe Mail-Adressen ein oder tragen Sie den Namen anderer Gruppen ein um hierarchische Beziehungen zwischen den Mail-Verteilern mehrerer Gruppen zu realisieren. Drücken Sie dann auf den Schalter „Hinzufügen“ um die Adresse in den Verteiler aufzunehmen. Bitte beachten Sie, daß diese zusätzlichen Adressen manuell gepflegt werden müssen. Verweist ein Eintrag z.B. auf eine andere Gruppe und diese Gruppe wird gelöscht, so muß diese manuell aus dem Verteiler gelöscht werden.

Über den Schalter „Gruppe löschen“ können Sie die komplette Gruppe löschen. Der Schalter wird bei den vier Systemgruppen nicht angeboten.

Betätigen Sie den Schalter „OK“ um wieder in die Anzeige aller verfügbaren Gruppen zu wechseln.

9.3.2.1. Sonderbedeutung der Gruppe system-mail

Die Gruppe system-mail enthält alle Benutzer die über ein lokales Mail-Konto verfügen. Wenn Sie also eine Mail an die Gruppe system-mail versenden, erhält diese jeder lokale Benutzer der die Möglichkeit hat Mails zu erhalten.

Im praktischen Gebrauch werden Sie diese Gruppe möglicherweise lieber als Mail-Verteiler „alle“ adressieren wollen. Legen Sie dazu eine neue Gruppe „alle“ an. Tragen Sie in dieser Gruppe nun als „zusätzliche Mail-Adresse im Verteiler alle“ den Gruppennamen „system-mail“ ein.

Wird ein Benutzer aus der Gruppe system-mail gelöscht, bleibt sein Postfach erhalten und kann weiter genutzt werden, wenn der Benutzer zu einem späteren Zeitpunkt wieder zu dieser Gruppe hinzugefügt wird. Das Postfach wird hingegen gelöscht, wenn der Benutzer vollständig aus der Benutzerverwaltung entfernt wird.

9.3.2.2. Sonderbedeutung der Gruppe system-proxy

In der Gruppe system-proxy sind alle Benutzer enthalten für die ein Konto im Proxy-Cache angelegt wurde. Die dieser Gruppe zugeordneten Proxy-Listen finden daher bei allen Benutzern Anwendung die sich am Proxy-Cache anmelden. Zusätzlich werden die Proxy-Listen der Gruppe System-proxy auch auf Anfragen angewendet, für die keine Benutzeranmeldung stattgefunden hat oder wenn der angemeldete Benutzer auf dem DEFENDO unbekannt ist (bei externer Anmeldung z.B. an LDAP). Benutzen Sie daher die Proxy-Listen der Gruppe System-proxy, wenn Sie die Benutzeranmeldung vollständig abgeschaltet haben bzw. um den Zugriff auf Seiten zu reglementieren für die die Benutzeranmeldung deaktiviert wurde.

9.4. Proxylisten

9.4.1. Allgemeines zu Proxylisten

Im Menüpunkt Proxylisten definieren Sie URL-Filterlisten für den Internetzugriff über den DEFENDO Proxy-Cache. Diese Listen werden dann mit Hilfe der Gruppenverwaltung auf bestimmte Benutzer angewendet.
Jede Proxyliste beinhaltet dabei die Möglichkeit, selbst eine Negativliste und eine Positivliste von Domains zu erstellen. Darüber hinaus lassen sich beliebige Dateierweiterungen sperren. Ferner ist eine URL-Datenbank mit verschiedenen inhaltlichen Kategorien integriert. Der Zugriff auf bestimmte Kategorien aus dieser Datenbank läßt sich einschränken. Der Zugriff ausschließlich auf die Positivlisten begrenzen. Eine Proxyliste kann zeitlich immer, während oder außerhalb der Arbeitszeiten aktiv sein. Die Arbeitszeiten lassen sich dabei frei definieren. Es ist schließlich auch möglich, einzelne Proxylisten vorübergehend zu deaktivieren.

Hinweis:

Die Proxylisten überprüfen jede Anfrage eines Browsers anhand der angeforderten Adresse (URL). Die Überprüfung der Anwort eines Webservers im Internet wird von den Proxylisten nicht durchgeführt. Dies ist Aufgabe der DEFENDO-Komponente Proxy-Virenscan und Tagfilter.

Ein Benutzer kann mehreren Gruppen zugeordnet sein. Diesen Gruppen wiederum können mehrere Proxylisten zugeordnet werden. Ein Benutzerzugriff unterliegt damit der Summe der Proxylisten aus mehreren Gruppen. Die Überprüfung ob ein Zugriff gestattet wird erfolgt in der nachfolgend beschriebenen Reihenfolge und endet sobald die Adresse in einer der Listen gefunden wird: Zunächst wird der Zugriff gegen alle Negativlisten geprüft. Anschließend erfolgt die Prüfung gegen alle Positivlisten. Es folgt dann ein Vergleich mit allen gesperrten Dateierweiterungen und der Summe der gesperrten Datenbankkategorien. Ist in mindestens einer anzuwendenden Proxyliste der Zugriff ausschließlich auf die Positivlisten begrenzt, so wird der Zugriff abgewiesen, andernfalls akzeptiert.

Ein abgewiesener Zugriff wird über eine entsprechende Seite dem Benutzer angezeigt. Lediglich Einträge aus der Datenbankkategorie „Werbung“ werden auf ein transparentes Bild umgelenkt. Auf diese Weise werden Werbebanner von den in der Datenbank gelisteten Adressen ausgeblendet.

Ist die Benutzerauthentifizierung gegenüber dem Proxy-Cache nicht aktiviert, so finden lediglich die Proxylisten der Systemgruppe systemproxy anwendung. Die Benutzerauthentifizierung wird wie auch der URL-Filter selbst über die Proxy-Cache Konfiguration aktiviert.

Achtung:

Der URL-Filter muß über die Proxy-Cache Konfiguration aktiviert werden. Andernfalls haben die Proxylisten keine Wirkung.

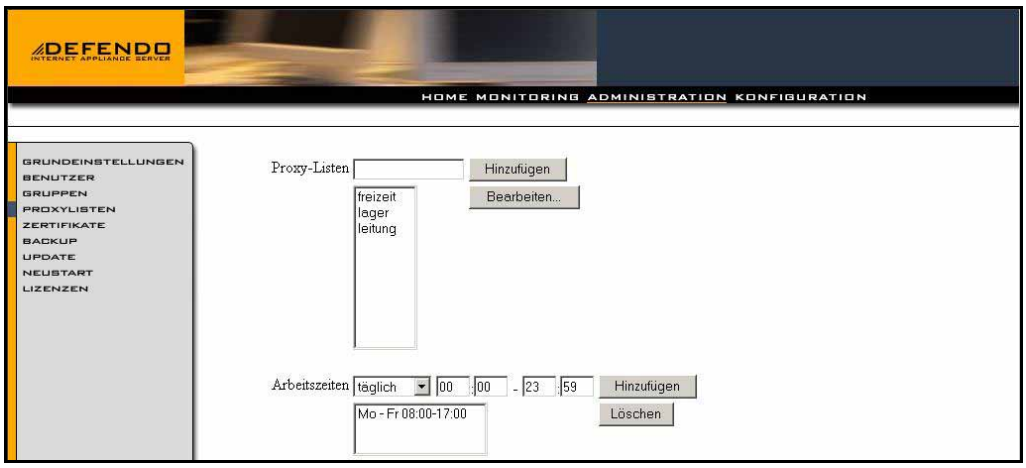
9.4.2. Anlegen / Ändern von Proxylisten

Zum Erstellen einer neuen Proxyliste tragen Sie bitte in das entsprechende Feld den Namen der Liste ein und bestätigen Sie Ihre Eingabe mit dem Schalter „Hinzufügen“.

Bitte beachten Sie bei der Vergabe der Listennamen, dass die Verwendung von Umlauten sowie Leerzeichen nicht zugelassen wird. Es dürfen außerdem nur Kleinbuchstaben und Ziffern verwendet werden. Als Sonderzeichen sind nur der Bindestrich (-), der Punkt (.) und der Unterstrich (_) zulässig. Eine Beschränkung der Länge besteht nicht.

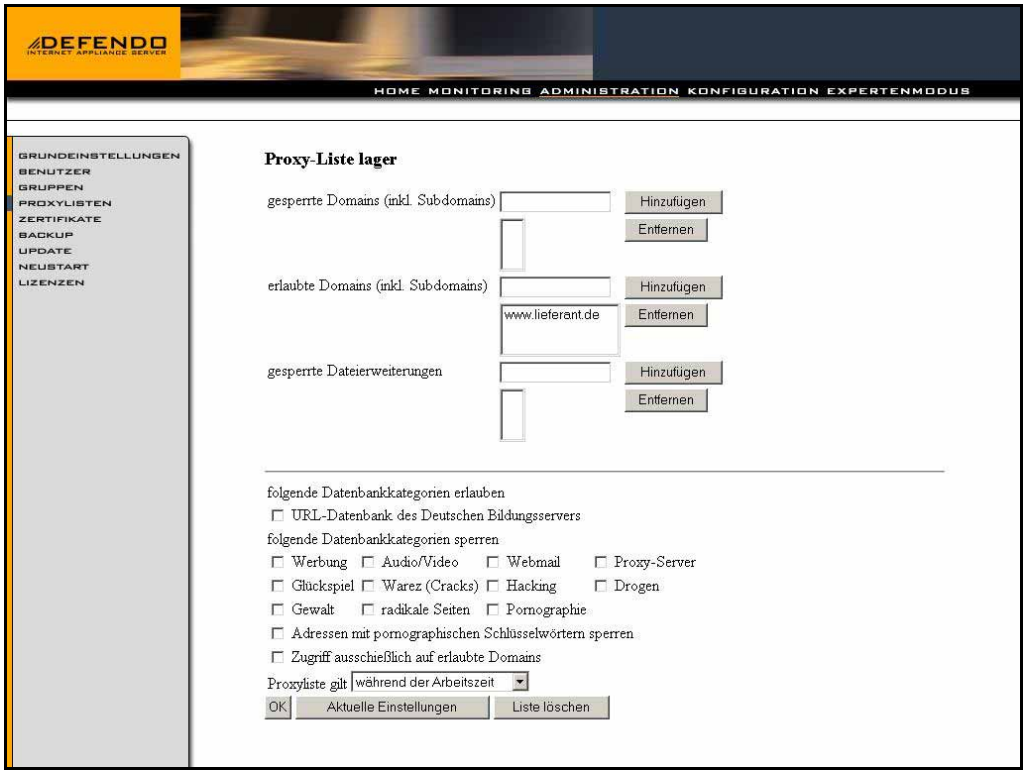
Markieren Sie eine bereits angelegte Proxyliste und drücken Sie auf „Bearbeiten“ um die Einstellungen dieser Liste zu verändern oder die Liste zu löschen.

Im unteren Bereich der Maske haben Sie die Möglichkeit, die Zeitintervalle zu konfigurieren, die als Arbeitszeit gelten sollen. Wählen Sie die gewünschten Wochentagsbereiche aus und geben Sie die zugehörigen Uhrzeiten ein. Drücken Sie dann auf „Hinzufügen“ um ein weiteres Zeitintervall als Arbeitszeit gelten zu lassen. Wählen Sie ein bereits eingetragenes Zeitintervall aus der Liste und drücken Sie auf „Entfernen“ um einen Zeitbereich nicht mehr als Arbeitszeit gelten zu lassen.



9.4.3. Proxyliste konfigurieren

In dieser Maske haben Sie die Möglichkeit, die Einschränkungen der Proxyliste zu konfigurieren:



Gesperrte Domains

Tragen Sie hier Domains ein, auf die kein Zugriff mehr möglich sein soll. Dies beinhaltet auch Subdomains. Ist z.B. der Zugriff auf domain.com gesperrt, so ist damit auch z.B. der Zugriff auf www.domain.com und ftp://ftp.domain.com gesperrt. Groß- und Kleinschreibung werden nicht unterschieden. Alle Einträge werden in Kleinbuchstaben umgewandelt. Tragen Sie eine Domain ein und drücken Sie auf den Schalter „Hinzufügen“ um eine Domain zu sperren, wählen Sie eine Domain aus der Liste und drücken Sie auf „Entfernen“ um den Zugriff auf eine Domain wieder freizugeben.

Erlaubte Domains

Auf alle hier eingetragenen Domains inklusive Subdomains ist der Zugriff erlaubt. Die Hinweise zu den gesperrten Domains gelten hier entsprechend. Benutzen Sie diesen Eingabebereich um Domains die

fälschlicherweise in einer der URL-Datenbanken gesperrt werden freizugeben, um den Zugriff auf nachfolgend gesperrte Dateierweiterungen für bestimmte Server freizugeben oder eine Positivliste von Adressen zu definiern wenn Sie beabsichtigen für die Gruppe ausschließlich den Zugriff auf freigegebene Domains zu erlauben.

Gesperrte Dateierweiterungen

Tragen Sie eine Dateierweiterung ein und drücken Sie auf „Hinzufügen“ um den Zugriff auf Adressen mit dieser Dateierweiterung zu sperren oder wählen Sie eine Erweiterung aus der Liste und drücken Sie den Schalter „Entfernen“ um den Zugriff wieder freizugeben. Die Angabe der Dateierweiterung kann im Format ext, .ext oder *.ext erfolgen. Groß- und Kleinschreibung werden nicht unterschieden. Alle Einträge werden in Kleinbuchstaben umgewandelt. Bitte beachten Sie, daß die angesprochene URL ausschließlich anhand des Namens und nicht Ihres Inhalts mit der Liste der Dateierweiterungen verglichen wird.

Datenbankkategorien erlauben

Wählen Sie die gewünschten Kategorien aus, auf die Zugriff gewährt werden soll. Lediglich die Einträge unter der Rubrik „gesperrte Domains“ haben Vorrang vor den Einträgen die in dieser Datenbank geführt werden. Insbesondere finden die gesperrten Dateierweiterungen keine Anwendung auf Adressen in dieser Datenbank.

Datenbankkategorien sperren

Wählen Sie die gewünschten Kategorien aus, auf die der Zugriff gesperrt werden soll.

Adressen mit pornographischen Schlüsselwörtern sperren

Wir dieser Schalter aktiviert, so werden bestimmte Schlüsselwörter in der angesprochenen URL gesucht, die auf pornographischen Inhalt hindeuten und in diesem Falle der Zugriff gesperrt. Bitte beachten Sie, daß der eigentliche Inhalt der Seite nicht geprüft wird.

Zugriff ausschließlich auf erlaubte Domains

Ist dieser Schalter aktiv, so kann bei Anwendung dieser Proxyliste ausschließlich auf freigegebenen Adressen zugegriffen werden.

Proxyliste gilt

Wählen Sie hier aus, wann die Einschränkungen der gewählten Proxyliste angewendet werden sollen. Eine Proxyliste kann immer, während oder außerhalb der Arbeitszeiten angewendet werden. Die Einstellung „nie (Liste deaktiviert)“ ermöglicht es Ihnen ferner, eine Proxyliste un-

wirksam zu machen ohne diese Löschen zu müssen oder aus der Gruppenzuordnung zu entfernen.

Drücken Sie den Schalter „OK“ um Änderungen in den Optionen zu aktivieren. Mit Hilfe des Schalters „Liste löschen“ wird die gesamte Liste einschließlich aller Einträge gelöscht.

9.4.4. Hinweis zu den Datenbankkategorien

Die verwendete Datenbank für gesperrte Kategorien wurde weitgehend automatisch mit Hilfe von sogenannten Robots erstellt. Mit falsch zugeordneten Einträgen in den Listen ist daher zu rechnen. Aufgrund der Vielzahl der Internet-Adressen und deren Dynamik ist in der Datenbank stets auch nur ein Bruchteil der tatsächlich vorhandenen Seiten zu den Kategorien eingetragen.

Vom „Deutschen Bildungsserver“ wurde uns freundlicherweise die Online-Ressourcen-Datenbank zur Verfügung gestellt. Aus dieser wurde automatisch eine Positivliste generiert die weitgehend den Zugriff auf die Online-Ressourcen ermöglicht. Links von den Online-Ressourcen aus auf andere Server oder Serverbereiche werden jedoch im allgemeinen nicht abgedeckt.

9.5. Zertifikate

Das Menü Zertifikate erlaubt es, neue RSA-Schlüssel für die verschiedenen verschlüsselten Dienste des DEFENDO zu erstellen. Ferner kann hier der RSA-Schlüssel des DEFENDO VPN-Servers exportiert und importiert werden.

Im oberen Bereich der Maske werden die Daten angezeigt die in alle neu erstellten Zertifikate für den DEFENDO aufgenommen werden. Um diese zu ändern, drücken Sie bitte die Schaltfläche „Ändern“ und geben Sie die gewünschten Daten ein. Mit „OK“ werden diese dann als neue Voreinstellung übernommen.

Im unteren Bereich der Maske werden eine Reihe möglicher Aktionen angeboten. Wählen Sie die gewünschte Aktion aus und drücken Sie auf die „Weiter“ Schaltfläche um weitere Einstellungen für die gewünschte Aktion vorzunehmen.

9.5.1. Neues HTTPS-Server Zertifikat

Dieses Zertifikat wird für den verschlüsselten Zugriff auf die Administrationsoberfläche des DEFENDO verwendet. Stellen Sie das Zertifikat auf die Adresse aus, mit der Sie in Ihrem Web-Browsers üblicherweise auf die Adminstrationsoberfläche zugreifen. Dies ist in der Regel die IP-Adresse oder der Rechnername Ihres DEFENDO. Sie können das Zertifikat allerdings auch auf einen beliebigen von Ihnen definierten Wert ausstellen. Wählen Sie die passende Option aus und drücken Sie auf die Schaltfläche „Zertifikat erstellen“ um ein neues selbstsigniertes HTTPS-Server Zertifikat mit einer Gültigkeitsdauer von einem Jahr auszustellen.

9.5.2. Neues Mail-Server Zertifikat

Dieses Zertifikat wird für den verschlüsselten Zugriff auf POP3-/ IMAP4-Mail-Konten verwendet. Ferner benutzt es der Mail-Server des DEFENDO bei der verschlüsselten Nachrichtenübermittlung. Stellen Sie das Zertifikat auf die Adresse aus, mit der der POP3-, IMAP4- bzw. SMTP-Server üblicherweise angesprochen wird. Ist der direkte Zugriff aus dem Internet auf diese Serverdienste möglich, so ist dies ist in der Regel der DNS-Name unter dem das System aus dem Internet adressiert wird. Erfolgt der Zugriff nur aus dem internen LAN, ist hier normalerweise die IP-Adresse oder der Rechnername Ihres DEFENDO zu verwenden. Sie können das Zertifikat allerdings auch auf einen beliebigen anderen von Ihnen definierten Wert ausstellen. Wählen Sie die passende Option aus und drücken Sie auf die Schaltfläche „Zertifikat erstellen“ um ein neues selbstsigniertes Mail-Server Zertifikat mit einer Gültigkeitsdauer von einem Jahr auszustellen.

9.5.3. Neues VPN-Server Zertifikat

Dieses Zertifikat wird vom VPN-Server des DEFENDO verwendet. Üblicherweise wird das Zertifikat auf die IP-Adresse ausgestellt, unter der der DEFENDO aus dem Internet erreichbar ist. Bei dynamischer IP-Adresse können Sie alternativ z.B. den Rechnernamen des DEFENDO verwenden. Oder stellen Sie das Zertifikat auf einen beliebigen anderen von Ihnen definierten Wert aus. Wählen Sie die passende Option aus und drücken Sie auf die Schaltfläche „Zertifikat erstellen“ um ein neues selbstsigniertes Zertifikat mit einer Gültigkeitsdauer von einem Jahr auszustellen.

Sie können auch ein Zertifikat für den VPN-Server im PKCS12-Format importieren. Wählen Sie dazu mit Hilfe der „Durchsuchen“-Schaltfläche eine PKCS12-Datei von der Festplatte Ihres Computers aus, geben Sie das Import-Paßwort ein und drücken Sie dann auf „Schlüsselpaar importieren“ um die PKCS12-Datei an den DEFENDO zu übermitteln. In der Folgemaske werden Ihnen die Daten des in der PKCS12-Datei enthaltenen Zertifikates angezeigt. Mit „Fertigstellen“ wird das Zertifikat vom VPN-Server des DEFENDO übernommen.

Achtung:

Nach der Änderung des VPN-Server Zertifikates muß der neue öffentliche Schlüssel an alle VPN-Clients und VPN-Server übermittelt werden, die über X.509-Zertifikat authentifiziert in Verbindung mit dem DEFENDO stehen.

9.5.4. VPN-Server-Zertifikat exportieren

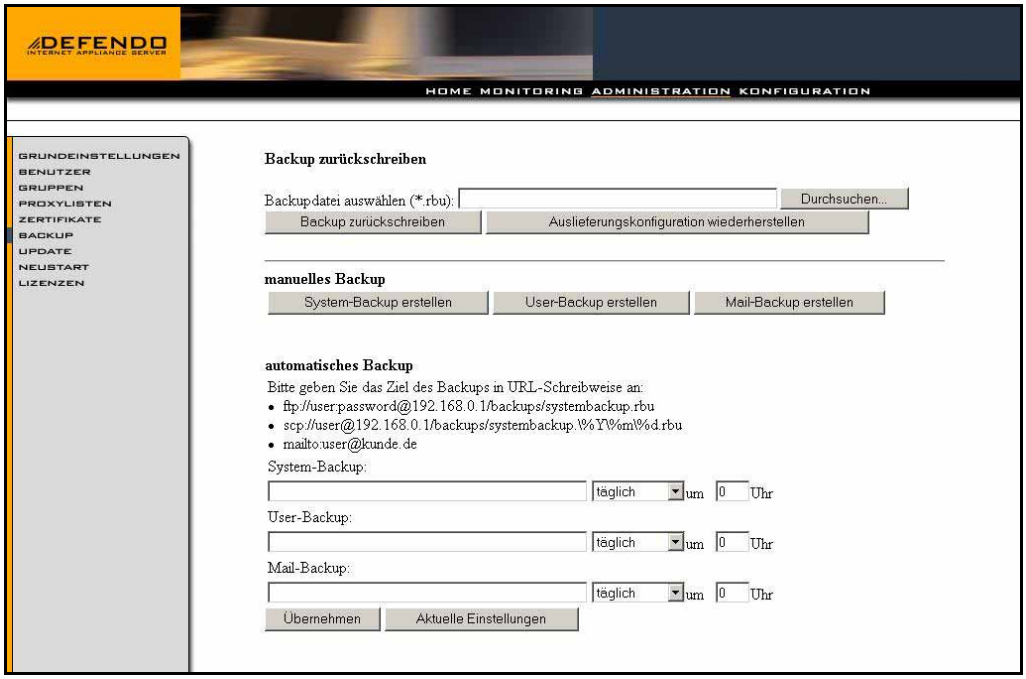
Das RSA-Schlüsselpaar des VPN-Servers kann zu Sicherungszwecken im PKCS12-Format exportiert werden. Bitte beachten Sie, daß dieser Export also auch den privaten Schlüssel enthält, der unbedingt geheim bleiben muß. Der private Schlüssel wird durch das anzugebende Export-Paßwort geschützt und kann nur mit diesem Paßwort wieder importiert werden. Drücken Sie auf „Schlüsselpaar exportieren“ um die Schlüssel auf Ihren PC herunterzuladen. Wir empfehlen, die PKCS12-Datei sicher aufzubewahren (z.B. auf Disketten in einem Safe).

Über den Schalter „Public key exportieren“ kann der öffentliche Schlüssel des DEFENDO im PEM-Format heruntergeladen werden. Der öffentliche Schlüssel muß VPN-Kommunikationspartnern übermittelt wer-

den, wenn die gegenseitige Authentifizierung über X.509-Zertifikate erfolgt. In diesem Bereich wird auch das Subject und die Gültigkeitsdauer des DEFENDO Zertifikates angezeigt.

9.6. Backup

Mit diesem Menüpunkt ist es möglich, die Einstellungen des DEFENDO zu sichern bzw. zurückzuschreiben oder sogar die Werkseinstellungen wiederherzustellen.



Gerade bei einem Defekt des Gerätes ist dies äußerst hilfreich. Es brauchen dann nur die IP-Adresse des DEFENDO eingestellt und die Sicherungsdateien zurückgespielt werden.

9.6.1. Einstellungen zurückschreiben

Zum Zurücksichern dient der obere Teil der Maske. Mit Hilfe des Schalters „Durchsuchen“ geben Sie über eine Funktionsmaske des Windows-Explorers an, in welchem Pfad sich die zurücksichernde Datei befindet. Dies kann die Datei für die Systemdateien sein (Systembackup.rbu) oder aber auch die Sicherungsdatei der Benutzer (Userback.rbu). Ferner ist ein Rücksichern des Postfaches (Posteingang) des POP3/IMAP4-Servers möglich (Mailbackup.rbu). Sollten die Namen der

Dateien von Ihnen geändert worden sein, so wählen Sie bitte diese entsprechend. Nach der Auswahl der Datei wird der Pfad in der Maske im Feld neben dem Schalter „Durchsuchen“ angezeigt. Wenn der Schalter „Backup zurückschreiben“ gewählt wird, erscheint eine Abfrage des DEFENDO , um sicher zugehen, dass Sie diesen Schritt wirklich durchführen wollen.

Microsoft Internet Explorer
Sind Sie sicher, daß Sie das Backup zurückspielen wollen?
Hinweise für User- und Systembackups:
Es gehen hierbei alle Änderungen verloren,
die seit dem Erstellen dieses Backups vorgenommen wurden.
!!! Es wird empfohlen, zuvor ein Backup der aktuellen Einstellungen zu erstellen !!!
Hinweise für Mailbackups:
Es werden nur die Postfächer von den Benutzern zurückgespielt, deren Postfach nicht existiert.
Sie müssen also zuerst die entsprechenden Postfächer über Monitoring -> Mailserver löschen und dann das Backup einspielen.
OK
Abbrechen

Generell ist es vor den Zurückschreiben des Benutzer- bzw. des Systembackups empfehlenswert zuvor eine Sicherung der momentanen Einstellungen durchzuführen, da die aktiven Einstellungen vollständig mit denen aus dem Backup überschrieben werden.

Beim Zurückschreiben eines Mailbackups wird ein Postfach nur dann aus dem Backup übernommen, wenn der zugehörige Benutzer nach wie vor Mitglied der Benutzergruppe system-mail ist (siehe Kapitel 9.3.2.1) und das Postfach zuvor gelöscht wurde (siehe Kapitel 11.4). Postfächer von nicht mehr existierenden Benutzern bzw. von Benutzern die nicht mehr berechtigt sind Mail zu empfangen werden also nicht zurückgesichert. Ebenso ist gewährleistet, dass keine eMail aus dem aktuellen Posteingang verloren geht, da ein Postfach nur dann aus dem Backup übernommen wird, wenn das Postfach zum Zeitpunkt der Rücksicherung nicht existiert.

Hinweis:

Ein gelöschtes Postfach wird automatisch wieder angelegt sobald eine eMail an dieses Postfach zugestellt wird.

Nach der Bestätigung des Schalters „OK“ wird die von Ihnen gewählte Sicherung zurückgeschrieben.

9.6.2. Auslieferungskonfiguration wiederherstellen

In manchen Fällen ist es notwendig, die Ausgangskonfiguration (Werkseinstellungen) wiederherzustellen. Dazu dient der gleichlautende Schalter am unteren Ende dieser Maske.

Sobald dieser bedient wird, wird eine entsprechende Warnmeldung ausgegeben.

Microsoft Internet Explorer
Sind Sie sicher, daß Sie die Auslieferungskonfiguration wiederherstellen wollen?
VORSICHT:
Es gehen dabei alle Änderungen verloren,
die bis jetzt auf diesem System vorgenommen wurden.
HINWEIS:
Es wird empfohlen, daß zuvor ein Backup der aktuellen Einstellungen erstellt wird.
OK
Abbrechen

Auch hier wird empfohlen, vorher eine Sicherung durchzuführen. Sollte die IP-Adresse des DEFENDO geändert worden sein, so ist der DEFENDO nach Bestätigung des Schalters „OK“ nicht mehr erreichbar. Zur erneuten Konfiguration des DEFENDO starten Sie bitte im Kapitel 6.

9.6.3. Sichern der Konfiguration

Zum Sichern der Konfiguration dient der untere Abschnitt dieser Maske. Hier finden Sie alle benötigten Optionen. Es werden drei Sicherungen unterscheiden: Systemeinstellungen (System-Backup), Benutzereinstellungen (User-Backup) inklusive der Passwörter und Benutzerpostfächer (Mail-Backup). Halten Sie diese Sicherungsdateien stets unter Verschluss, da sie in falschen Händen auch gelesen werden können!

Das User-Backup beinhaltet die Einstellungen, die Sie über das System-Menü in den Bereichen Benutzer, Gruppen und Proxylisten vornehmen. Das System-Backup enthält alle weiteren Einstellungen. Im Mail-Backup sind alle Postfächer (Posteingang) des POP3/IMAP4-Servers enthalten.

Zum manuellen Sichern des System-Backups verwenden Sie bitte den gleichlautenden Schalter. Nach dem Anklicken des Schalter erhalten Sie eine Maske, die einen Dateidownload anzeigt.

Voreingestellt ist die Auswahl „Datei auf Datenträger speichern“. Sollte dies nicht der Fall sein, so wählen Sie bitte diese Option an. Bestätigen Sie Ihre Angabe mit dem „OK“-Schalter. Es öffnet sich nun ein Fenster des Windows-Explorers, mit dessen Hilfe Sie in der Lage sind, die Datei „Sysbackup.rbu“, die vom DEFENDO generiert wird, an einen beliebigem Platz auf Ihrem PC oder besser auf Ihrem Server ablegen können. Dies ist sinnvoll, damit diese Datei von der in der Regel nächtlichen Tagessicherung mit gesichert wird. Der Dateiname kann natürlich auch geändert werden.

Verfahren Sie mit dem User-Backup und dem Mail-Backup auf die gleiche Weise. Die hierbei generierten Dateien nennen sich „Userbackup.rbu“ bzw. „Mailbackup.rbu“. Auch diese Namen können beliebig geändert werden.

Die Erstellung der Backups kann auch automatisch erfolgen. Tragen Sie dazu die Zieladresse des Backups in URL-Schreibweise in den dafür vorgesehenen Feldern zum System-, User- bzw. Mail-Backup ein. Wählen Sie ferner den zeitlichen Rhythmus und die Uhrzeit zu der das Backup erstellt werden soll. Ein monatliches Backup wird jeweils am ersten des Monats durchgeführt, ein wöchentliches am Montag. Verwenden Sie folgendes Format bei der Angabe der URL:

- **Backup via eMail:**

  Das Backup kann per Mail an eine beliebige Adresse zugestellt werden. Die URL dazu hat das Format mailto:user@domain (z.B. mailto:admin@muster.de). Bitte beachten Sie, daß die Daten dabei unverschlüsselt übertragen werden.

- **Backup via FTP:**

  Das Backup läßt sich auf einen FTP-Server ablegen. Verwenden Sie dazu folgende URL:

  ftp://login:passwort@server/pfad/dateiname

  Die Anmeldung an den FTP-Server erfolgt mit der angegebenen Benutzerkennung und dem angegebenen Paßwort. Der Servername kann in Form einer IP-Adresse oder eines gültigen DNS-Namens eingegeben werden. Die Angabe eines Pfades auf dem Server kann entfallen. Soll das Backup jedoch in ein Unterverzeichnis abgelegt werden, so muß dieses Verzeichnis bereits auf dem FTP-Server angelegt sein. Das Backup wird mit dem angegebenen Dateinamen erstellt. Dieser darf spezielle Zeichenkombinationen enthalten, die dann durch das Datum des Backups ersetzt werden können. Als Zeichenkombinationen stehen zur Verfügung:

\%Y: Jahr 4-stellig (z.B. 2001)

\%y : Jahr 2-stellig (z.B. 01)

\%m: Monat (von 01 bis 12)

\%d: Tag (von 01 bis 31)

\%H: Stunde (von 00 bis 23)

\%M: Minute (von 00 bis 59)

\%S: Sekunde (von 00 bis 59)

\%U: Woche des Jahres (Werte von 00 bis 53)

\%w: Tag der Woche (0 für Sonntag bis 6 für Samstag)

\%j: Tag im Jahr (von 000 bis 366)

Im folgenden Beispiel erfolgt die Anmeldung an den ftp-Server 192.168.0.1 mit Benutzername backup und Paßwort geheim. Das Backup wird stets unter dem Namen systembackup.rbu angelegt und daher jedesmal überschrieben:

ftp://backup:geheim@192.168.0.1/systembackup.rbu

Im folgenden Beispiel wird das Backup in einem Unterverzeichnis auf dem Server ftp://ftp.kunde.de erstellt und enthält sowohl Tag als auch Monat im Namen. Ein Backup würde somit erst im folgenden Jahr wieder überschrieben werden, sofern es dann am gleichen Datum erstellt wird:

ftp://backup:geheim@ftp.kunde.de/backup/system-\%m.\%d.rbu

Die Daten werden beim Backup mit ftp unverschlüsselt übertragen.

Sollte das Backup nur über einen vorgeschalteten FTP-Proxy möglich sein, so fügen Sie bitte ein Leerzeichen und eine FTP-Proxy-Spezifikation an:

ftpproxy://Proxykennung:Proxypasswort@Servername:Port.

- **Backup via Secure-Shell / Secure-Copy**

  Das Backup läßt sich schließlich auch verschlüsselt an einen Secure-Shell-Server mit Hilfe von scp übermitteln. Auf dem Secure-Shell-Server liegen die Daten danach unverschlüsselt vor. Die Ziel-URL wird in folgendem Format angegeben:

  scp://login@server/pfad/dateiname.

  Die Authentifizierung des Benutzers erfolgt bei dieser Methode nicht über ein Paßwort sondern mit Hilfe des RSA-Keys Ihres DEFENDO. Der Secure-Shell-Server ist entsprechend zu konfigurieren. Das Verfahren arbeitet ansonsten entsprechend dem Backup mit FTP. Das Beispiel 2 aus dem FTP-Backup

Backup mit FTP. Das Beispiel 2 aus dem FTP-Backup hätte mit scp realisiert folgendes Aussehen:

scp://backup@ftp.kunde.de/backup/sytem-\%m.\%d.rbu

Achtung:

Das Backup enthält aus Sicherheitsgründen keine RSA-Schlüsselpaare. Sollten Sie VPN-Verbindungen zu VPN-Servern bzw. -Clients mit Authentifizierung über X.509-Zertifikaten unterhalten, so ist das Backup insoweit unvollständig. Sichern Sie darum das VPN-Server-Zertifikat des DEFENDO mit der entsprechenden Export-Funktion separat (vgl. Kapitel 9.5.4).

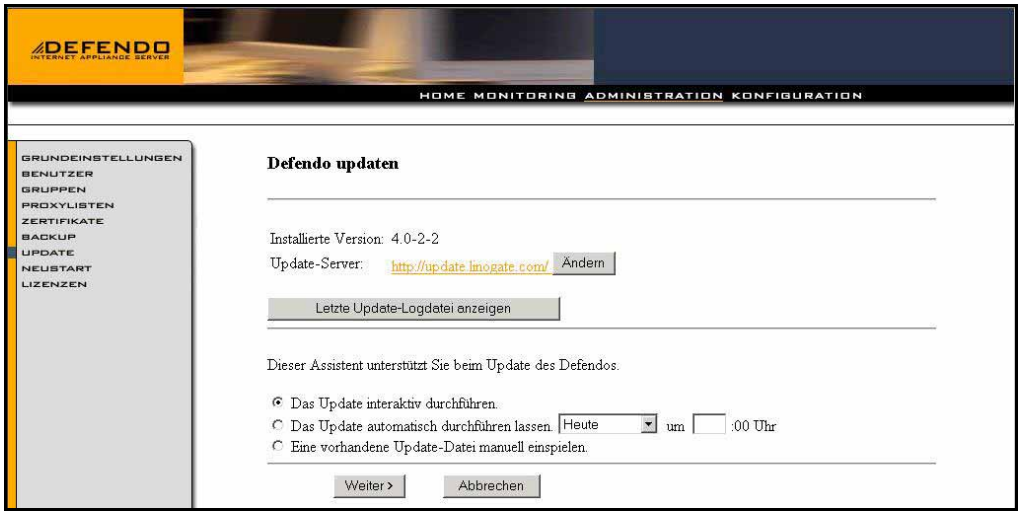
9.7. Update

Hier können vorhanden Updates für Ihren DEFENDO eingespielt werden. Überprüfen Sie bitte regelmäßig auf unsere Homepage unter www.linogate.de/update ob sich dort neue Updates befinden.

Zudem erhalten Sie hier Informationen über die installierte Version Ihres DEFENDO sowie des installierten Update-Levels. Diese Angaben sind bei Inanspruchnahme des Supports (siehe Kapitel 14) eventuell notwendig.

Das Einspielen eines Updates dauert in der Regel einige Minuten und löst ggf. selbständig einen Neustart des Systems aus. Bitte beachten Sie die Hinweise in den README-Dateien zum jeweiligen Update.

Die Versionsinformation sollte nach einem Update einen neuen Wert anzeigen. Sollte dies nicht der Fall sein, so wenden Sie sich bitte an den technischen Support (siehe Kapitel 14).



Update-Server

Um den Update-Vorgang weitgehend automatisieren zu können, läßt sich die Adresse eingeben, von der die Updates bezogen werden sollen. Um diese Adresse anzupassen, drücken Sie auf die „Ändern“-Schaltfläche. Geben Sie in der folgenden Maske die neue Adresse in URL-Schreibweise an. Updates können mit Hilfe der Protokolle http, ftp oder scp bezogen werden.

Sollte der http- bzw. ftp-Download nur über einen vorgeschalteten Proxy möglich sein, so fügen Sie bitte ein Leerzeichen und eine Proxy-Spezifikation an: proxy://Servername:Serverport. Erfordert der Proxy eine Benutzeranmeldung, so verwenden Sie bitte folgendes Format: proxy://Benutzerkennung:Passwort@Servername:Serverport. Sollte es sich bei dem Proxy um einen reinen ftp-Proxy handeln, so ersetzen Sie bitte proxy:// durch ftpproxy://.

Mit „Übernehmen“ wird der geänderte Update-Server gespeichert.

Letzte Update-Logdatei anzeigen

Mit Hilfe dieses Schalters können Sie Meldungen einsehen, die beim letzten Update erzeugt wurden. Bei Problemen nach dem Einspielen eines Updates geben diese Meldungen ggf. Aufschluß über die Ursache des Problems.

Update interaktiv durchführen

Wählen Sie diesen Optionsschalter und drücken Sie auf „Weiter“ um das Update weitgehend automatisiert durchzuführen. Die einzelnen Schritte können dabei bestätigt werden, der Update-Vorgang läßt sich jederzeit abbrechen. Zunächst prüft der DEFENDO ob auf dem Update-Server neuere Updates zur Verfügung stehen. Durch wiederholtes drü-

cken der „Weiter“-Schaltfläche werden diese nacheinander eingefügt, bis keine aktuellen Updates mehr zur Verfügung stehen.

Update automatisch durchführen

Wählen Sie diesen Optionsschalter und geben Sie den gewünschten Tag und die Uhrzeit ein zu der das Update durchgeführt werden soll. Drücken Sie dann auf „Weiter“. Der DEFENDO prüft dann, ob auf dem Update-Server neue Updates zur Verfügung stehen. Drücken Sie auf „Fertigstellen“ um das Update zeitgesteuert durchzuführen. Sollten Sie als Tag „heute“ und als Uhrzeit eine bereits vergangene Zeit eingegeben haben, wird das Update am folgenden Tag um diese Zeit ausgeführt. Sobald ein automatisches Update eingeplant ist, erscheint eine entsprechende Meldung unter dem Menüpunkt Update. Hier ist es möglich, das automatische Update zu löschen.

Vorhandene Update-Datei manuell einspielen

Falls die Update-Datei in Form einer *.rup-Datei bereits lokal bei Ihnen vorliegt, können Sie diese Datei auch manuell einspielen. Dies ist vor allem für größere Updates sinnvoll, die auch auf CD ausgeliefert werden können. Aktivieren Sie dazu den entsprechenden Optionsschalter und drücken Sie auf „Weiter“.

Klicken Sie bitte auf den Schalter „Durchsuchen“ um die einzuspielende *.rup-Datei, die z.B. auf der Festplatte Ihres PC gespeichert ist, auszuwählen. Die entsprechende Datei wird nach Bestätigung im Feld neben dem Schalter „Durchsuchen“ angezeigt.

Starten Sie das Update schließlich mit dem Schalter „Fertigstellen“. Die ausgewählte Datei wird dann an den DEFENDO übermittelt und installiert.

9.8. Neustart

Sollte ein Neustart des DEFENDO notwendig sein, oder das Gerät abgeschaltet werden müssen, verwenden Sie bitte diese Option dafür.

Nach Anwahl des Menüpunktes „Neustart“ unter den Administration-Menü erhalten die Möglichkeit zwischen zwei Aktionen auszuwählen:

System herunterfahren

Fährt nach Anwahl dieser Aktion und nach Bestätigung des Schalters „Ausführen“ das System herunter und schaltet es nach Möglichkeit aus.

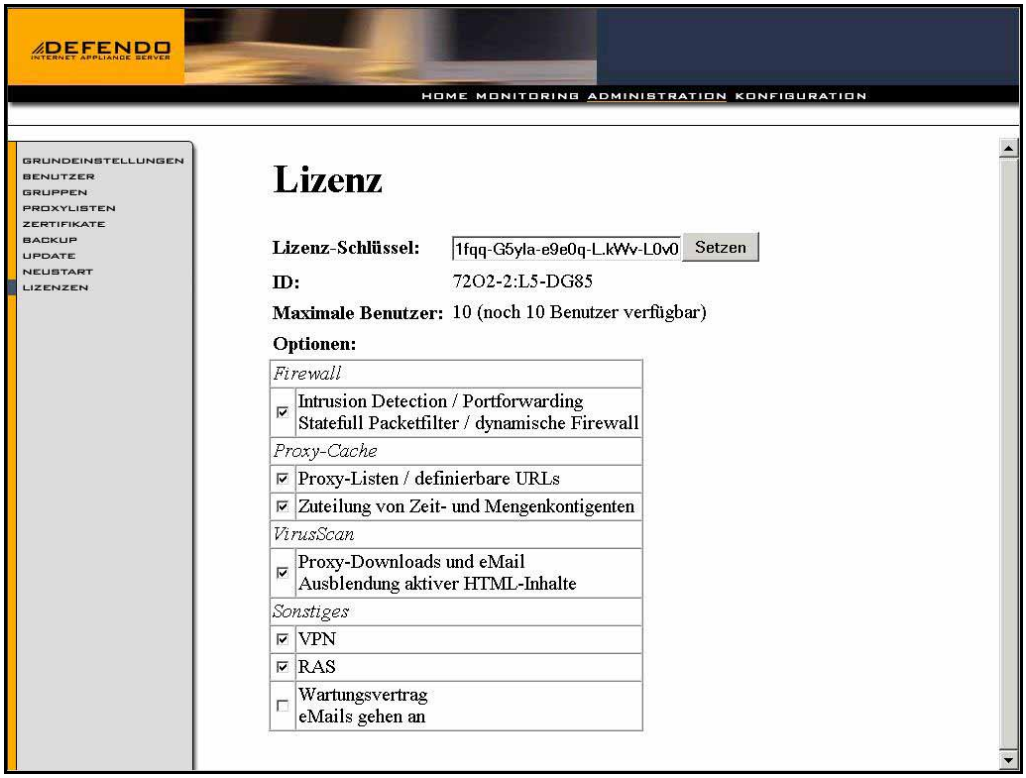
System herunterfahren und neu starten

Diese Aktion führt einen Neustart des Systems aus. Wählen Sie die Option und bestätigen Sie den Schalter „Ausführen“. In diesem Fall kann es bis zu 5 Minuten dauern, bis der DEFENDO wieder einsatzbereit ist.

In beiden Fällen wird eine entsprechende Sicherheitsabfrage getätigt. Bestätigen Sie diese mit Schalter „OK“.

9.9. Lizenzen

In diesem Bereich ist der Lizenzschlüssel des DEFENDO hinterlegt. Die mit diesen Schlüssel verfügbaren Benutzer, die Geräte ID und die freigeschalteten Optionen können hier abgefragt werden.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
GRUNDEINSTELLUNGEN
BENUTZER
GRUPPEN
PROXYLISTEN
ZERTIFIKATE
BACKUP
UPDATE
NEUSTART
LIZENZEN
Lizenz
Lizenz-Schlüssel:
1fqq-G5yla-e9e0q-L.kWv-L0v0
Setzen
ID:
72O2-2:L5-DG85
Maximale Benutzer:
10 (noch 10 Benutzer verfügbar)
Optionen:
Firewall
Intrusion Detection / Portforwarding
Statefull Packetfilter / dynamische Firewall
Proxy-Cache
Proxy-Listen / definierbare URLs
Zuteilung von Zeit- und Mengenkontigenten
VirusScan
Proxy-Downloads und eMail
Ausblendung aktiver HTML-Inhalte
Sonstiges
VPN
RAS
Wartungsvertrag
eMails gehen an

10. Das Hauptmenü „Home“

Das Hauptmenü „Home“ gibt kurze Hinweise zur Orientierung auf der DEFENDO -Oberfläche. Im linken Menü finden Sie ferner den Kontaktbereich, der die Daten Ihres Support-Ansprechpartners enthält. Der Bereich „Benutzer“ ist als Einziger für alle Benutzer zugänglich, denen das Recht „system-web“ in der Benutzerverwaltung gegeben wurde. Alle Benutzer können hier ihre Passwörter ändern, sofern der Administrator das entsprechende Recht erteilt hat. Ferner kann der Benutzer Mail-Weiterleitungen zu seinem Postfach bearbeiten.

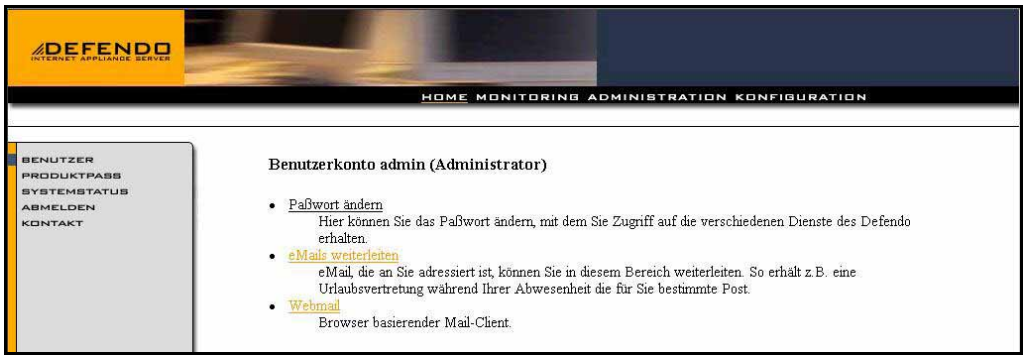
Nach Anwahl des Hauptmenüs „Home“ wird die Eingangsmaske dieses Menüs angezeigt.

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
BENUTZER
PRODUKTPASS
SYSTEMSTATUS
ABMELDEN
KONTAKT
Willkommen
auf der Benutzeroberfläche von DEFENDO
Home:
Der Menüpunkt Benutzer aus der linken Menüleiste ermöglicht es berechtigten Benutzern, Ihr Kennwort zu ändern und Einstellungen für das eigene Mailkonto vorzunehmen. Die Menüpunkte Produktpass und Systemstatus fassen wichtige Daten zu Ihrem DEFENDO zusammen.
Konfigurationsbereich:
Der Konfigurationsbereich bleibt dem Administrator vorbehalten. Hier läßt sich die Netzwerkkonfiguration an Ihr lokales Umfeld anpassen. Ferner können hier vielfältige Einstellungen an den verschiedenen Diensten des DEFENDO vorgenommen werden.

10.1. Benutzer

Wählen Sie zur Vergabe von neuen Passwörtern und E-Mail-Weiterleitungen den links angeordneten Untermenüpunkt „Benutzer“. Nun wird der entsprechende Benutzer mit Hilfe des Anmeldungsfensters um Anmeldung gebeten. Im Anmeldefenster ist der Name und das Passwort des Benutzers einzugeben, der seine Einstellungen ändern möchte. Sollten Sie sich mit Ihrem Browser bereits als ein Benutzer an-

gemeldet haben und Sie wollen sich nun als ein anderer Benutzer anmelden, so benutzen Sie bitte zunächst die „Abmelden“-Funktion. Ist die Anmeldung erfolgreich durchgeführt, wird in das entsprechende Untermenü verzweigt und Sie erhalten folgende Auswahlmaske:

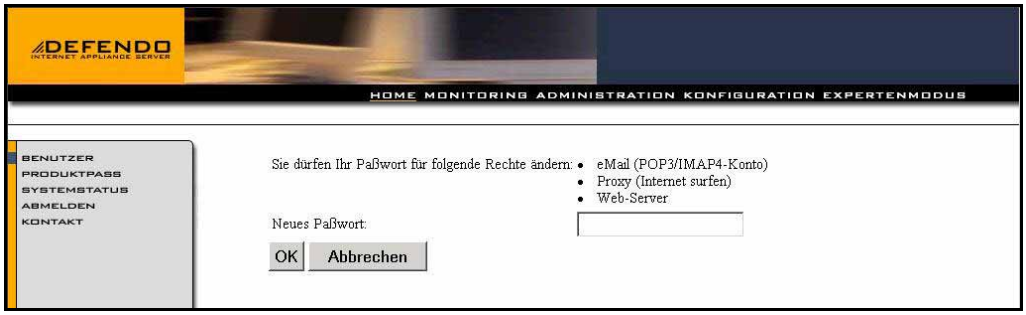

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
BENUTZER
PRODUKTPASS
SYSTEMSTATUS
ABMELDEN
KONTAKT
Benutzerkonto admin (Administrator)
Paßwort ändern
Hier können Sie das Paßwort ändern, mit dem Sie Zugriff auf die verschiedenen Dienste des Defendo erhalten.
eMails weiterleiten
eMail, die an Sie adressiert ist, können Sie in diesem Bereich weiterleiten. So erhält z.B. eine Urlaubsvertretung während Ihrer Abwesenheit die für Sie bestimmte Post.
Webmail
Browser basierender Mail-Client.

In dieser Maske ist auch der Zugriff auf den Webmail-Bereich möglich. Sie können jedoch auch direkt über die Adresse https://NAME_ODER_IP/webmail/ zugreifen.

10.1.1. Passwort ändern

Mit dieser Funktion können berechtigte Benutzer Ihr Passwort für zugeteilte Rechte ändern. Diese Änderung gilt für alle zugeteilten Rechte für die der Benutzer selbst das Passwort ändern darf. Für diese Rechte gilt dann das gleiche Passwort.

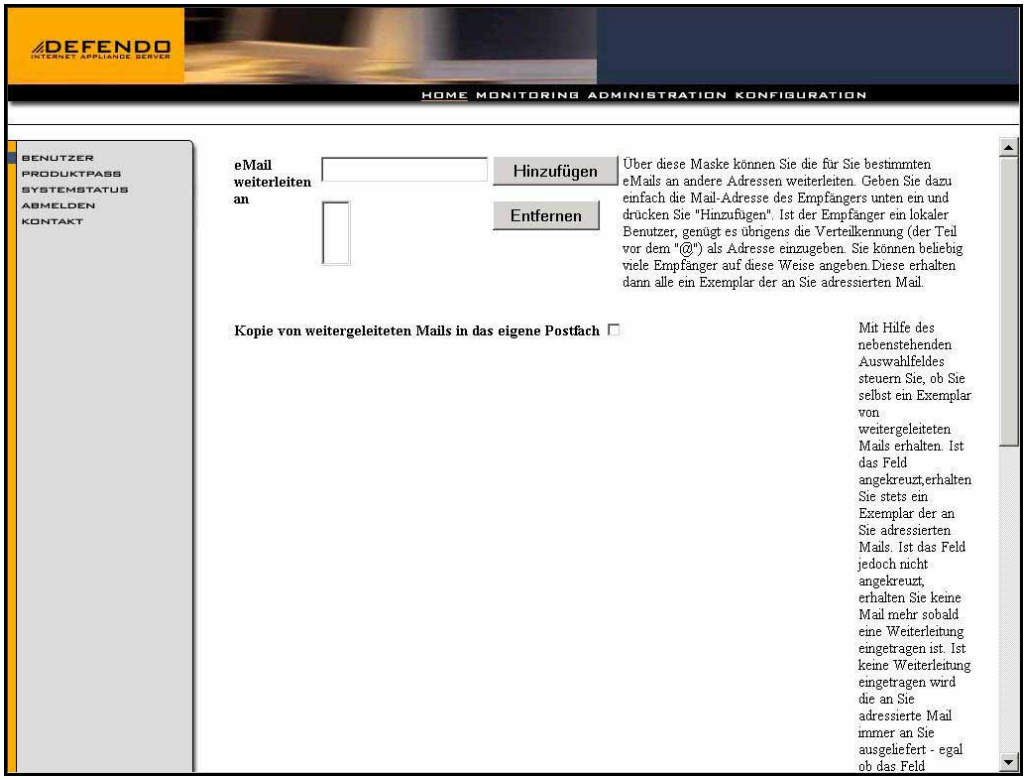
Wählen Sie hierzu in der Maske „Benutzer“ den Auswahlpunkt „Passwort ändern“ und Sie erhalten folgende Eingabemaske:



Ihnen werden nun die Dienste angezeigt, für die Sie eine Berechtigung haben. Tragen Sie im Eingabefeld „neues Passwort“ das Entsprechende ein und alle verfügbaren Dienste erhalten dieses Passwort. Bestätigen Sie Ihre Eingabe mit dem Schalter „OK“. Eine Sicherheitsabfrage für die Kennworteingabe erfolgt nicht, da dass Passwort in Klarschrift eingetippt wird. Sie gelangen nun wieder in die Ausgangsmaske.

10.1.2. Weiterleiten von E-Mails

E-Mails, die an den entsprechenden Benutzer adressiert sind, können in diesem Bereich weitergeleitet werden. So erhält z.B. eine Urlaubsvertretung während der Abwesenheit die für ihn bestimmte Post. Hat der Benutzer eine „anonyme“ E-Mail-Adresse bei einem Internetanbieter (z. B. Yahoo, GMX) könnte die Mail auch an diese Internet-Mail-Adresse weitergeleitet werden. Steht im Außendienst oder im Urlaub ein PC mit Internetzugang bereit, können von der ganzen Welt aus die E-Mails gelesen werden, die eigentlich an die Adresse in der Firma adressiert waren.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
BENUTZER
PRODUKTPASS
SYSTEMSTATUS
ABMELDEN
KONTAKT
eMail weiterleiten an
Hinzufügen
Entfernen
Über diese Maske können Sie die für Sie bestimmten eMails an andere Adressen weiterleiten. Geben Sie dazu einfach die Mail-Adresse des Empfängers unten ein und drücken Sie "Hinzufügen". Ist der Empfänger ein lokaler Benutzer, genügt es übrigens die Verteilkennung (der Teil vor dem "@") als Adresse einzugeben. Sie können beliebig viele Empfänger auf diese Weise angeben.Diese erhalten dann alle ein Exemplar der an Sie adressierten Mail.
Kopie von weitergeleiteten Mails in das eigene Postfach
Mit Hilfe des nebenstehenden Auswahlfeldes steuern Sie, ob Sie selbst ein Exemplar von weitergeleiteten Mails erhalten. Ist das Feld angekreuzt,erhalten Sie stets ein Exemplar der an Sie adressierten Mails. Ist das Feld jedoch nicht angekreuzt, erhalten Sie keine Mail mehr sobald eine Weiterleitung eingetragen ist. Ist keine Weiterleitung eingetragen wird die an Sie adressierte Mail immer an Sie ausgeliefert - egal ob das Feld

Im Feld „E-Mails weiterleiten an“ ist die Mail-Adresse des Empfängers einzutragen. Drücken Sie den Schalter „Hinzufügen“. Ist der Empfänger ein lokaler Benutzer, genügt es übrigens die Verteilkennung (der Teil vor dem „@“) als Adresse einzugeben. Sie können beliebig viele Empfänger auf diese Weise angeben. Diese erhalten dann alle ein Exemplar von der an das aktuelle Postfach adressierten Mail.

Mit Hilfe des Optionfeldes „Kopie von weitergeiteten Mails in das eigene Postfach“ steuern Sie, ob stets auch ein Exemplar von eingehenden Mails in das lokale Postfach zugestellt werden soll. Ist das Feld jedoch nicht angekreuzt, erhält das entsprechende Postfach keine Mail mehr sobald eine Weiterleitung eingetragen ist. Ist keine Weiterleitung eingetragen, wird die an das aktuelle Postfach adressierte Mail immer in dieses Postfach ausgeliefert - egal ob das Feld angekreuzt ist oder nicht.

Es ist möglich auf eingehende Mails automatisch eine Antwort zu generieren um z.B. den Empfang zu bestätigen oder im Falle einer längeren Abwesenheit den Absender der Mail darüber zu benachrichtigen. Als Antwort kann eine beliebige Textnachricht gesendet werden, die in das Eingabefeld unter „automatische Antwort auf eingehende Mails“ eingetragen werden kann. Ist hier kein Text hinterlegt, so wird auch keine automatische Antwort generiert.

> *Hinweis:*
>
> *Eine automatische Antwort wird für jede eMail generiert, die in das entsprechende Postfach zugestellt wird. Es werden also auch Antwortmails erzeugt, wenn die Mail über einen Verteiler (Gruppe) an das entsprechende Postfach ausgeliefert wurde. Es werden hingegen keine Antwortmails erzeugt, wenn die Mails weitergeleitet werden ohne daß eine Kopie in das eigene Postfach zugestellt wird.*

10.1.3. Webmail

Der Zugriff auf den browserbasierenden Mail-Client ist für alle Benutzer möglich, die Mitglied der Gruppe sytem-mail sind. Die Mitgliedschaft in der Gruppe system-web ist nicht erforderlich. Benutzer die nicht Mitglied von system-web sind können folglich auch nicht auf den Menüpunkt Home -> Benutzer zugreifen. Diese Benutzer verwenden daher bitte den direkten Link https://NAME_ODER_IP/webmail/ um auf Webmail zuzugreifen.

Hinweis:

Da der Zugriff auf Webmail an die Mitgliedschaft in der Gruppe system-mail gekoppelt ist, ist auch das für die Gruppe system-mail vergebene Passwort zu verwenden.

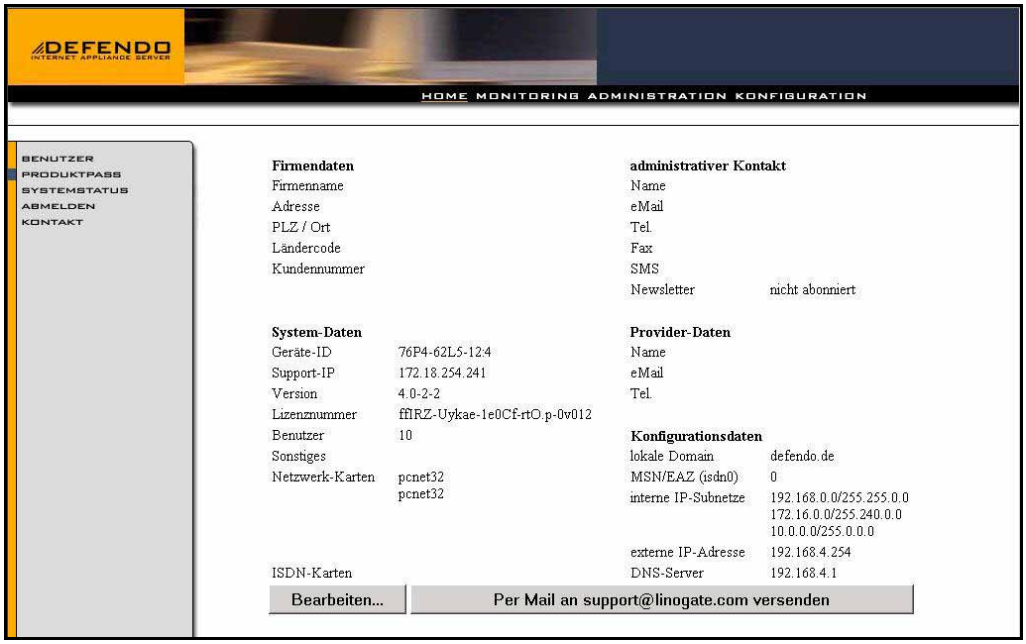
Um mit einem Browser Webmail nutzen zu können, muß im Browser JavaScript aktiviert sein. Ferner müssen Cookies zugelassen werden.

Achtung:

Webmail ist nicht Bestandteil des Backup. Alle Einstellungen, Addressen, Termine, eMails, ... werden nicht gesichert. Einzige Ausnahme ist der Ordner Eingang, der über das Mail-Backup gesichert werden kann.

10.2. Produktpass

Unter diesem Menüpunkt werden die wichtigsten Informationen zu Ihrem System, dem administrativen Ansprechpartner und Ihrem Provider zusammengefaßt. Mit Hilfe des Schalters „Bearbeiten...“ können Sie die Firmendaten, den administrativen Kontakt und die Providerdaten ändern.



Die Daten des Produktpasses lassen sich über den entsprechenden Schalter per Mail an uns versenden. Sie ermöglichen es uns so, noch schneller und gezielter bei Schwierigkeiten reagieren zu können.

10.3. Systemstatus

Dieser Menüpunkt gibt einen kurzen Überblick über die aktuellen Eckdaten Ihres Systems. Halten Sie diese Daten bereit, wenn Sie sich an Ihren Support wenden.

Im unteren Bereich der Maske führt das System bei jedem Aufruf dieser Seite eine Selbstdiagnose durch. Sofern etwas ungewöhnliches erkannt wird, ist hier eine entsprechende Meldung zu sehen. Über den Schalter „Netzwerkanalyse“ wird eine kurze Diagnose der Internetanbindung durchgeführt. Nutzen Sie diese Funktion um Problemen beim Internetzugriff auf die Spur zu kommen.

10.4. Abmelden

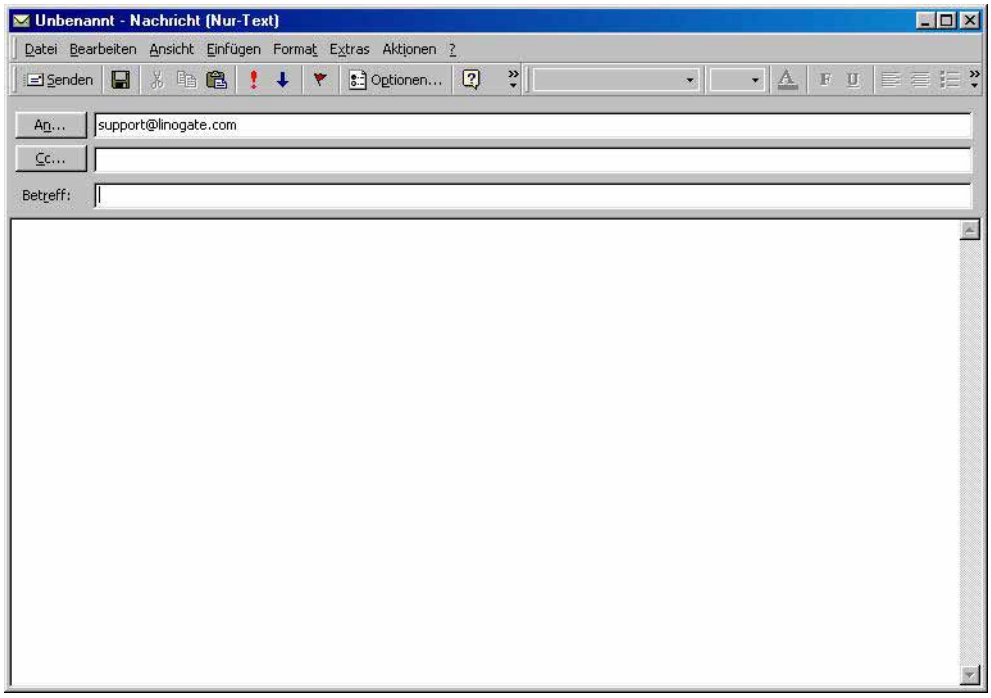
Betätigen Sie diesen Schalter, wenn Sie sich von der Administrationsoberfläche des DEFENDO abmelden möchten. Alternativ muß der Browser komplett beendet werden (alle Browser-Fenster müssen geschlossen werden). Das Schließen des aktuellen Fensters oder das Wechseln des Browsers auf eine andere Internet-Adresse ist nicht ausreichend, um den erneuten Zugriff auf die Administrationsoberfläche des DEFENDO zu verhindern. Ohne Abmeldung könnte so z.B. während einer kurzen Abwesenheit ein Unbefugter auf die DEFENDO Administrationsoberfläche wechseln und dort ohne erneute Anmeldung zugreifen.

Wenn Sie den Menüpunkt „Abmelden“ anwählen und der Browser öffnet ein Anmeldefenster, so sind Sie bereits abgemeldet. Andernfalls wird zunächst angezeigt, als welcher Benutzer Sie aktuell angemeldet sind. Wenn Sie hier den Schalter „Abmelden“ drücken, öffnet der Browser ein Anmeldefenster. Geben Sie hier kein Kennwort oder ein falsches Kennwort ein und bestätigen Sie. Sie sind erst dann abgemeldet, wenn die Meldung „Sie sind abgemeldet“ erscheint.

10.5. Kontakt

Über diesen Menüpunkt erhalten Sie Informationen, wie Sie mit Ihrem autorisierten DEFENDO - Support (siehe Kapitel 14) in Kontakt treten können.

Er wird sich umgehend mit Ihrer Anfrage befassen und entsprechend reagieren.



11. Das Hauptmenü „Monitoring“

Dieser Menüpunkt beinhaltet einige Überwachungsfunktionen, um sich über den System-Status Ihres DEFENDO zu informieren und mögliche Ursachen von Funktionsstörungen zu ergründen. Gerade diese Funktionen erleichtern Ihnen und gegebenenfalls uns die Fehlersuche.

Auch erfahren Sie den Zustand der verfügbaren Dienste mit der Möglichkeit diese zu starten, neu zu starten sowie zu beenden. Zudem können Sie hier die Statistiken des Proxy-Cache-Servers und des Web-Servers einsehen.

Nach Anwahl des Hauptmenüs „Monitoring“ wird die Eingangsmaske dieses Menüs angezeigt.

Im Auswahlmenü auf der linken Seite der Eingangsmaske finden Sie nachfolgende Einträge. Zur Aktivierung dieser klicken Sie bitte den entsprechenden Menüeintrag mit der Maus. Der DEFENDO wechselt dann in das entsprechende Untermenü. Alle möglichen Menüpunkte werden nun der Reihe nach beschrieben:

11.1. Dienste

Ihnen wird nach Anwahl dieses Menüpunktes eine Liste sämtlicher Dienste des DEFENDO angezeigt. Hierbei wird angezeigt, ob die entsprechenden Dienste laufen, oder nicht. Der Bildschirm ist in folgende Tabellenspalten eingeteilt:

Dienst: Zeigt Ihnen den Namen des Dienstes an.

Status: Zeigt an, ob der Dienst gestartet und bereit ist (ok) oder der entsprechende Dienst nicht gestartet bzw. nicht verfügbar ist (gestoppt). Die verfügbaren Dienste sind zum Teil abhängig von der Ausstattung Ihres DEFENDO .

Autostart: Befindet sich in dem Kästchen ein Haken, so wird dieser Dienst bei jedem Start des DEFENDO automatisch gestartet.

Befehle: Ermöglicht das sofortige Starten, Beenden sowie einen Neustart eines Dienstes.

Hinweis:

Wenn ein Dienst nicht gestartet ist, stehen dessen Funktionen auch nicht zur Verfügung. Manche Dienste sind Optionen, d. h. sie müssen extra erworben werden und sind nicht Bestandteil der Grundversion des DEFENDO . Wenden Sie sich bei gewünschten Erweiterungen an Ihren Support (siehe Kapitel 14).

11.1.1. Automatisches Starten von Diensten

Soll ein Dienst in Zukunft immer automatisch gestartet werden, so setzen Sie bitte in der Spalte „Autostart“ einen Haken neben dem entsprechenden Dienst und bestätigen Sie den Schalter „Übernehmen“ am Ende der Seite. Der Dienst wird nun bei jedem Systemneustart automatisch gestartet.

Sollen Dienste nicht mehr automatisch mit dem Systemneustart ausgeführt werden, so entfernen Sie bitte den Haken in der Spalte „Autostart“ und drücken Sie auf Übernehmen am Ende der Seite. Der Dienst wird nun beim nächsten Systemstart nicht mehr automatisch gestartet.

11.1.2. Sofortbefehle für Dienste

Um Dienste ohne einen Neustart beeinflussen zu können, wurden die Möglichkeiten „Starten“, „Beenden“ und „Neustart“ zur Verfügung ge-

stellt. Bitte vergewissern Sie sich, in welchen Zustand der betreffende Dienst sich befindet.

- **Starten**
  Dient zum Starten eines Dienstes, der noch nicht gestartet ist. Dies kann jedoch nur erfolgen, wenn für den entsprechenden Dienst benötigte Angaben zur Verfügung stehen.

- **Beenden**
  Bei Anwahl dieses Punktes kann ein gestarteter Dienst beendet werden. Sollte ein Haken bei „Autostart“ gesetzt sein, so wird dieser Dienst beim nächsten Neustart wieder gestartet.

- **Neustart**
  Bei Problemen mit bestimmten Diensten ist manchmal ein Neustart hilfreich. Bei Konfigurationssänderungen muß kein Neustart durchgeführt werden. Dieser wird vom DEFENDO automatisch durchgeführt.

In allen drei Fällen muß nach der Auswahl des Befehls, der Schalter „Befehl ausführen“ neben dem entsprechenden Dienst ausgeführt werden. Eine Sicherheitsabfrage erfolgt hierbei nicht.

Nachfolgend erhalten Sie eine Kurzbeschreibung der verfügbaren Dienste und deren Funktionen:

11.1.3. Der Dienst „Ethernet“

Ist verantwortlich, für die Netzwerkschnittstelle des DEFENDO . Da dieser Dienst extrem wichtig ist kann er nur neu gestartet werden. Zur nachträglichen Änderung bzw. Modifikation verwenden Sie bitte den Konfigurations-Assistenten „LAN-Anbindung“ oder lesen Sie im Kapitel 12.1.1 nach.

11.1.4. Der Dienst „ISDN“

Dieser Dienst ist notwendig, für die Fernwartung, die Anwahl Ihres Providers für den Internetzugang und Mailabholung sowie für die Einwahl möglicher RAS-Zugänge. Zur Konfiguration der Fernwartungsfunktion verwenden Sie bitte den Konfigurations-Assistenten „Fernwartung“ (siehe Kapitel 7.2) oder schlagen Sie im Kapitel 12.1 nach.

11.1.5. Der Dienst „ADSL / PPP over Ethernet“

Ist nur verfügbar, wenn Sie über ADSL-Wählleitung am Provider bzw. einer anderen Gegenstelle angebunden sind. Zur Konfiguration nutzen Sie bitte den Konfigurations-Assistenten zur Internet-Anbindung (siehe Kapitel **7.3**) oder schlagen Sie im Kapitel 12.1 nach.

11.1.6. Der Dienst VPN / IPSec

Dieser Dienst ermöglicht die Verschlüsselung zwischen zwei Stellen, die Daten miteinander austauschen. Hier wird angezeigt, ob VPN (Virtual Privat Network) aktiv ist. Für weitere Informationen hierüber lesen Sie bitte das Kapitel 12.1.6.

11.1.7. Der Dienst „Firewall“

Der Firewalldienst ist immer aktiv. Dies sehen Sie daran, dass der Dienst nicht beendet werden kann. Die Firewall verhindert während einer bestehenden Verbindung ins Internet Einburchversuche in Ihr LAN sowie andere nicht zugelassene Zugriff. Hierbei sind oft spezielle Einstellungen notwendig, die im Kapitel 12.2 beschrieben sind.

11.1.8. Der Dienst „dynamische Firewall“

Die dynamische Firewall erkennt bestimmte Angriffsmuster und Verbindungen die nicht angefordert wurden (stateful Packet Filter). Beim starten dieses Dienstes erhalten Sie im allgemeinen keine Rückmeldung durch den Browser aufgrund des stateful Packet Filterings. Alle bestehenden TCP-Verbindungen die über den DEFENDO abgewickelt werden, werden ebenfalls unterbrochen. Es sind spezielle Einstellungen notwendig, die im Kapitel 12.2 beschrieben sind.

11.1.9. Der Dienst „Intrusion Detection“

Die Intrusion Detection überwacht TCP/IP-Pakete anhand einer Signatur-Datenbank auf verdächtige Inhalte und gibt in einer Log-Datei entsprechende Warnungen aus. Es sind spezielle Einstellungen notwendig, die im Kapitel 12.2 beschrieben sind.

11.1.10. Der Dienst „DHCP-Server“

Der DHCP-Dienst vergibt an Geräte im LAN eigenständig TCP/IP-Adressen, wenn er aktiv ist. Er kann auch als „Secondary-DHCP-Server“ fungieren, d. h. er vergibt erst nach der wiederholten Anfrage eine TCP/IP-Adresse an ein Gerät, dass eine Adresse verlangt bzw. benötigt. Dies kann sehr nützlich sein, wenn der erste DHCP-Server ausgefallen ist. Weitere Informationen zu diesem Dienst finden Sie im Kapitel 12.3.

11.1.11. Der Dienst „DNS-Server“

Mit Hilfe dieses Dienstes können Sie den Domain-Name-Server des DEFENDO konfigurieren. Dieser Dienst ist für die Abbildung zwischen Namen und IP-Adressen im Internet erforderlich. Auf diesen Dienst bauen weitere Dienste des DEFENDO auf, weshalb der DNS-Dienst in jedem Falle gestartet sein sollte. Informationen zur Konfiguration dieses Dienstes finden Sie im Kapitel 12.4.

11.1.12. Der Dienst „Proxy-Cache“

Wird für den komfortablen Internetzugang benötigt. Er ist auch für die Abfrage der Benutzer bei der Verwendung des Internets zuständig. Auch die Zwischenspeicherung von Internetseiten wird durch diesen Dienst erledigt. Bitte lesen Sie in diesem Handbuch auch das Kapitel 12.5 für weitere Einstellungsmöglichkeiten.

11.1.13. Der Dienst „Mail-Server“

Mit Hilfe dieses Dienstes ist sichergestellt, dass Ihre E-Mails auch Ihren Empfänger erreichen. Für die Abholung von E-Mails innerhalb des LAN ist der Dienst POP3 (siehe nächsten Abschnitt) zuständig. Hinweise für Einstellungen können im Kapitel 12.6 nachgelesen werden.

11.1.14. Der Dienst „POP3 / FTP“

Dieser Dienst startet eine Reihe von Internet-Diensten auf dem DEFENDO. Dazu gehören unter anderem der Telnet-Server, der POP3-

und IMAP4-Server sowie der FTP-Server. Über POP3 oder IMAP4 werden Mails von den Mail-Konten des DEFENDO abgeholt. Der FTP-Dienst ermöglicht das Up- sowie Downloaden von Dateien direkt auf den DEFENDO.

11.1.15. Der Dienst „HTTP-Server“

Der Http-Server-Dienst ermöglicht den Zugriff auf den Internet- bzw. den Intranet-Web-Server des DEFENDO. Erläuterungen zu den hier erforderlichen Einstellungen finden Sie im Kapitel 12.8.

11.1.16. Der Dienst „DEFENDO -Konfiguration“

Auch dieser Dienst lässt sich nicht beenden. Er stellt die Formulare zur Verfügung, in die Sie Ihre Konfigurationseingaben in Ihrem Browser für den DEFENDO machen. Ihre Eingaben werden durch diesen Dienst verarbeitet.

11.1.17. Der Dienst „Windows-Freigaben“

Durch Einsatz dieses Dienstes können bestimmte Verzeichnisse des DEFENDO als Windows-Freigabe angesteuert werden. Er erscheint dann auch in der Netzwerkumgebung in einem Windows- bzw. einem Novell-Netzwerk. Somit können Dateien und Verzeichnisse auf dem DEFENDO via Explorer direkt verwaltet werden. Wie Sie diesen Dienst konfigurieren wird im Kapitel 12.10 beschrieben.

11.1.18. Der Dienst „Zeitsteuerung“

Der Dienst Zeitsteuerung ist für die zeitgesteuerte Ausführung von Programmen erforderlich. Er wird z.B. bei der Generierung von Statistiken oder der zeitgesteuerten Abholung von Mails verwendet.

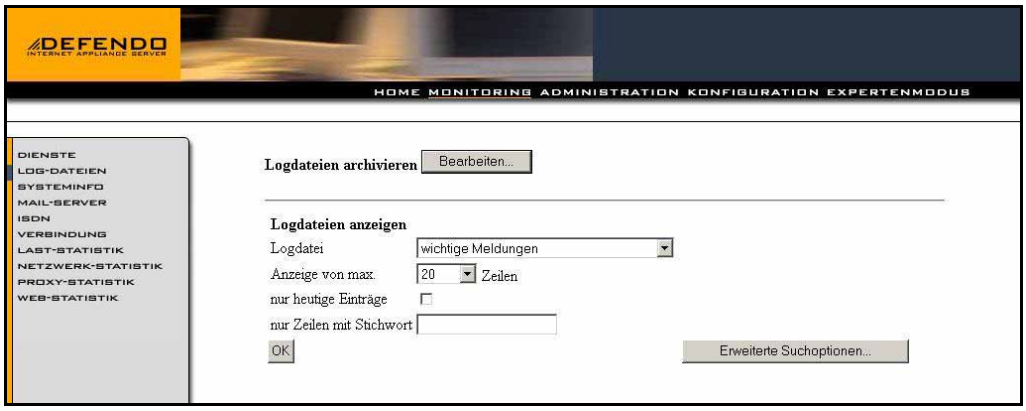
11.1.19. Der Dienst „System-Logging“

Beinhaltet die Protokollierung sämtlicher Systemeigenschaften, die über „Monitoring – LOG-Dateien“ (siehe Kapitel 11.2) eingesehen werden können.

11.2. Log-Dateien

Unter dem Menüpunkt „Log-Dateien“ haben Sie die Möglichkeit, für bestimmte Bereiche die aufgelaufen System- und Fehlermeldungen des DEFENDO abzurufen. Gerade bei der Inanspruchnahme des Supports (siehe Kapitel 14) und bei der Suche nach Ursachen für Fehlfunktionen sind diese äußerst hilfreich.

Systemintern werden funktional oder nach Wichtigkeit gegliedert mehrere Logdateien geschrieben. Die Logdateien werden wöchentlich jeweils Sonntags um 00:00 Uhr archiviert. Soweit nicht anders angegeben werden bis zu 12 archivierte Dateien werden im System gehalten, danach werden diese automatisch gelöscht. Neben der Archivierung auf dem System selbst lassen sich bestimmte Log-Dateien im gleichen Zyklus automatisch extern auf einen FTP- oder Secure-Shell-Server gzip-komprimiert archivieren. Auch ein Versenden per eMail ist möglich, dies ist aufgrund der eventuellen Größe der Log-Dateien jedoch nicht zu empfehlen.



Die verfügbaren Log-Dateien im einzelnen:

- **Wichtige Meldungen**

  Wichtige Meldungen und Fehlermeldungen aus verschiedensten Bereichen des DEFENDO sowie Systemmeldungen während des Bootvorgangs

- **Meldungen**

  weitere Meldungen aus verschiedensten Bereichen

- **Mail**

  Aufzeichung der ein- und ausgehenden Mails, Meldungen des Mail-Servers sowie POP3- und IMAP4-Anmeldungen an den DEFENDO

- **Proxy-Cache Zugriffe**
  Zugriffe auf den Proxy-Cache des DEFENDO.
- **Proxy-Cache Meldungen**
  Meldungen des Proxy-Caches des DEFENDO.
- **Web-Server Zugriffe**
  Zugriffe auf den Internet-Web-Server des DEFENDO.
- **Web-Server Fehlerlog**
  Fehlermeldungen des Internet-Web-Servers des DEFENDO.
- **Intranet-Web-Server Fehlerlog**
  Fehlermeldungen des Intranet-Web-Servers des DEFENDO.
- **Debugging**
  Debugmeldungen generiert von Programmen, die auf dem DEFENDO laufen. Von diese Logdatei werden nur bis zu drei archivierte Versionen im System gehalten.

11.2.1. Log-Dateien archivieren

Drücken Sie bei „Log-Dateien archivieren“ den Schalter „Bearbeiten...“ um die automatische Archivierung der Log-Dateien zu konfigurieren. In der Folgemaske sehen Sie für die Log-Dateien die automatisch archiviert werden können jeweils ein Eingabefeld. Ist dieses Feld leer, so findet keine externe Archivierung statt. Andernfalls ist hier in URL-Schreibweise anzugeben, wie die Log-Datei archiviert werden soll. Bei der Archivierung mit FTP und Secure-Copy ist beim Dateinamen die Angabe von bestimmten Platzhaltern möglich, die beim Sichern durch z.B. Datum oder Wochennummer ersetzt werden.

- **Archivierung via eMail:**
  Das Archiv kann per Mail an eine beliebige Adresse zugestellt werden. Die URL dazu hat das Format mailto:user@domain (z.B. mailto:admin@muster.de). Die Archivierung via eMail ist nicht zu empfehlen, da die Log-Dateien recht umfangreich werden können.
- **Archivierung via FTP:**
  Das Backup läßt sich auf einen FTP-Server ablegen. Verwenden Sie dazu folgende URL:

  ftp://login:passwort@server/pfad/dateiname

Die Anmeldung an den FTP-Server erfolgt mit der angegebenen Benutzerkennung und dem angegebenen Paßwort. Der Servername kann in Form einer IP-Adresse oder eines gültigen DNS-Namens eingegeben werden. Die Angabe eines Pfades auf dem Server kann entfallen. Soll das Backup jedoch in ein Unterverzeichnis abgelegt werden, so muß dieses Verzeichnis bereits auf dem FTP-Server angelegt sein. Das Backup wird mit dem angegebenen Dateinamen erstellt. Dieser darf spezielle Zeichenkombinationen enthalten, die dann durch das Datum des Backups ersetzt werden können. Als Zeichenkombinationen stehen u.a. zur Verfügung:

\%Y: Jahr 4-stellig (z.B. 2001)

\%y : Jahr 2-stellig (z.B. 01)

\%m: Monat (von 01 bis 12)

\%d: Tag (von 01 bis 31)

\%U: Woche des Jahres (Werte von 00 bis 53)

\%j: Tag im Jahr (von 000 bis 366)

Im folgenden Beispiel erfolgt die Anmeldung an den ftp-Server 192.168.0.1 mit Benutzername backup und Paßwort geheim. Das Backup wird stets unter dem Namen maillog.gz angelegt und daher jedesmal überschrieben:

ftp://backup:geheim@192.168.0.1/maillog.gz

Im folgenden Beispiel wird die Log-Datei in ein Unterverzeichnis auf den Server ftp://ftp.kunde.de kopiert und enthält sowohl Tag als auch Monat im Namen. Das Archiv würde somit erst im folgenden Jahr wieder überschrieben werden, sofern es dann am gleichen Datum erstellt wird:

ftp://backup:geheim@ftp.kunde.de/logfiles/maillog-\%m.\%d.gz

Sollte die Archivierung nur über einen vorgeschalteten FTP-Proxy möglich sein, so fügen Sie bitte ein Leerzeichen und eine FTP-Proxy-Spezifikation an:

ftpproxy://Proxykennung:Proxypasswort@Servername:Port.

- **Archivierung via Secure-Shell / Secure-Copy**

  Log-Dateien lassen sich schließlich auch verschlüsselt an einen Secure-Shell-Server mit Hilfe von scp übermitteln. Auf dem Secure-Shell-Server liegen die Daten danach unverschlüsselt vor. Die Ziel-URL wird in folgendem Format angegeben:

  scp://login@server/pfad/dateiname.

Die Authentifizierung des Benutzers erfolgt bei dieser Methode nicht über ein Paßwort sondern mit Hilfe des RSA-Keys Ihres DEFENDO. Der Secure-Shell-Server ist entsprechend zu konfigurieren. Das Verfahren arbeitet ansonsten entsprechend der Archivierung mit FTP. Das Beispiel 2 aus der FTP-Archivierung hätte mit scp realisiert folgendes Aussehen: scp://backup@ftp.kunde.de/logfiles/mail-\%m.\%d.gz

11.2.2. Log-Dateien anzeigen

Zur Anzeige von Log-Dateien wählen Sie zuerst die gewünschte Log-Datei aus. Für die meisten Log-Dateien stehen bereits vordefinierte Filter zur Verfügung, die nur bestimmte Nachrichten aus einer Log-Datei extrahieren. In der Auswahlliste sind diese eingerückt und stehen jeweils direkt unter der zugehörigen Log-Datei.

Die Anzeige ist normalerweise auf 20 Zeilen beschränkt. Sie können jedoch mit Hilfe des entsprechenden Auswahlfeldes auch eine andere Schranke wählen.

Ferner ist es möglich, die Anzeige ausschließlich auf Einträge zu beschränken, die am heutigen Tage erzeugt wurden.

Eine Stichwortsuche ist möglich. Ist im entsprechenden Feld ein Eintrag vorhanden, so werden nur die Zeilen der ausgewählten Log-Datei angezeigt, die die angegebene Zeichenfolge in irgendeiner Form enthalten. Suchmuster können hier im Stile der sog. „basic regular expressions“ eingegeben werden. Einige Beispiel:

- \| Oder-Verknüpfung

- . ein beliebiges Zeichen
- \. Ein Punkt
- [3-6X] die Ziffern 3, 4, 5, 6 oder ein X
- [^3-6X] ein Zeichen aber nicht 3, 4, 5, 6 oder X

So lässt sich z.B. nach den Monatsabkürzungen Jun und Jul auf folgende weisen suchen:

- Jun\|Jul
- Ju[nl]

Die Standardsuche findet stets ohne Beachtung der Groß- / Kleinschreibung statt. Archivierte Versionen der gewählten Log-Dateien werden dabei nicht durchsucht. Diese und weitere Parameter lassen sich jedoch über die „erweiterten Suchoptionen“ einstellen.

Zum Starten der Suche klicken Sie bitte auf den Schalter „OK“. Die aufgelaufenen Meldungen werden Ihnen in der Maske nun angezeigt. Je nach Größe der zu durchsuchenden Logdateien und der Anzahl der anzuzeigenden Zeilen kann dies einige Zeit in Anspruch nehmen.

Die Anzeige der Logdateien beginnt stets mit einer Zeile, die folgende Informationen enthält: Dateiname der ältesten durchsuchten Datei und den Zeitpunkt des ältesten Eintrags in dieser Datei, Dateiname der aktuellsten Logatei und Zeitpunkt des jüngsten Eintrags in dieser Datei. Läuft die Suche auch über archivierte Logdateien, so trägt die älteste Datei hinter dem Dateinamen einen Punkt und die Anzahl der Archivierungszyklen (Wochen bzw. Monate) die seit deren Archivierung vergangen sind.

11.2.3. Erweiterte Suchoptionen

Drücken Sie auf den Schalter „erweiterte Suchoptionen“ und Sie erhalten zu den zuvor beschriebenen Einstellmöglichkeiten weitere hinzu.

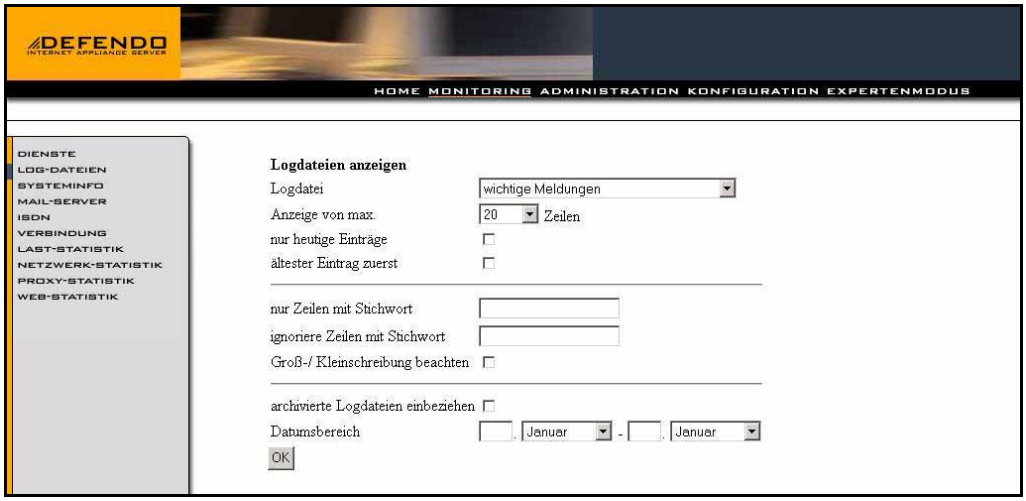
Normalerweise beginnt die Anzeige mit der aktuellsten Meldung der entsprechenden Logdatei. Dieses Verhalten kann auch umgekehrt werden. Bei der Anzeige „ältester Eintrag zuerst“ wird stets mit der ältesten Meldung der Logdatei begonnen. Enthält die Logdatei mehr Zeilen als angezeigt werden sollen, so werden die neueren Meldungen abgeschnitten.

Neben der Stichwortsuche ist es hier auch möglich, bestimmte Zeilen auszublenden. Geben Sie in das entsprechende Feld ein Suchmuster ein, so werden alle Zeilen auf die dieses Suchmuster passt ausgefiltert.

Groß- und Kleinschreibung wird bei der Suche im Normalfall nicht unterschieden, dieses Verhalten lässt sich jedoch über einen Schalter aktivieren.

Mit Hilfe des entsprechenden Schalters lässt sich die Suche auf die archivierten Logdateien des gewählten Typs erweitern. Bitte beachten Sie, dass je nach Größe und Anzahl der archivierten Logdateien der Suchaufwand beträchtlich steigen kann, wenn diese Option gewählt ist.

Um einen Bericht über einen definierten Zeitraum zu erstellen, lassen sich schließlich das Start- und / oder Enddatum des gewünschten Zeitraums einstellen. Wird beim Startdatum kein Tag angegeben, so sind alle beliebig alten Einträge enthalten. Wird beim Enddatum kein Tag angegeben so werden alle Einträge bis zum aktuellen Datum selektiert.



11.2.4. Besonderheiten bestimmter Log-Dateien

11.2.4.1. Meldungen – nur Firewall

In dieser Log-Datei werden fast alle Pakete aufgezeichnet, die durch die Standard-Firewall abgewiesen wurden. Die Ausgabe erfolgt zeilenweise und beginnt mit dem Datum und der Uhrzeit zu der das IP-Paket

vom DEFENDO registriert wurde. Die nächste wichtige Information ist die Firewall-Stufe in der das Paket aufgezeichnet wurde. Diese sind:

fw-in: Das Paket wurde vom DEFENDO empfangen

fw-fwd: Das Paket soll durch den DEFENDO hindurch geleitet werden

fw-out: Das Paket wollte den DEFENDO verlassen

Das nächste Feld gibt an, was mit dem Paket geschehen ist:

deny: das Paket wurde verworfen

rej: das Paket wurde verworfen, an den Absender wurde eine ICMP-Nachricht „no route to host“ gesendet.

acc: das Paket wurde akzeptiert. Akzeptierte Pakete werden im Normalfall nicht geloggt, so daß diese Meldung normalerweise nicht erscheinen sollte.

Im folgenden Feld wird die Schnittstelle angegeben, über die das Paket empfangen wurde (fw-in) bzw. über die das Paket den DEFENDO wieder verlassen sollte (fw-fwd und fw-out). Danach folgt das Layer3-Protokoll dieses Pakets. Die Protokolle TCP, UDP und ICMP werden mit Ihrem Namen dargestellt. Andere Protokolle mit dem Wert PROTO= gefolgt von der jeweiligen Protokollnummer. Bei ICMP wird zusätzlich der numerische ICMP-Typ an den Protokollnamen angefügt. Es folgen die IP-Adresse und der Quellport sowie die Zieladresse und der Zielport des Paketes. Adresse und Port sind dabei mit einem Doppelpunkt getrennt. Der Port wird nur bei den Protokollen TCP und UDP angezeigt. Die weiteren Felder enthalten unter anderem die Paketgröße des IP-Paketes, die Sequenz-Nummer und den Wert des TOS-Feldes.

11.2.4.2. Meldungen – nur DNS-Anfragen

Sofern im DNS-Server die Protokollierung der DNS-Anfragen aktiviert wurde, werden hier alle DNS-Anfragen an den DNS-Server des DEFENDO aufgezeichnet. Die Meldungen haben folgendes Format:

XX /Quelle/Anfrage/Anfragetyp

Die Quelle ist die IP-Adresse des anfragenden Clients, die Anfrage die Information nach der im DNS gesucht wird. Der Anfragetyp spezifiziert die gewünschte Information. Häufige Anfragetypen sind:

A: IP-Adresse zu Anfrage

PTR: DNS-Name zu Anfrage

MX:	Mail-Server zu Anfrage
NS:	Name-Server zu Anfrage
SOA:	Metainformationen zu Anfrage

11.2.4.3. Meldungen - nur ISDN-Leitungsstatus

Im ISDN-D-Kanal übermittelte Meldungen werden in dieser Log-Datei angezeigt. Sie geben Hinweis auf die Ursache von Verbindungsproblemen. Die Ausgabe erfolgt zeilenweise und beginnt mit dem Datum und der Uhrzeit, zu der die Meldung vom DEFENDO registriert wurde. Der Statuscode am Ende der Zeile beginnt bei Euro-ISDN (EDSS1) mit einem E, bei einer Standleitung mit L und bei nationalem ISDN (1TR6) ohne Buchstaben. Die folgenden zwei Stellen sagen aus, wo die Meldung generiert worden ist, während die letzten beiden Stellen den Grund der Meldung angeben. Die Meldungen unterscheiden sich je nach ISDN-Protokoll:

Euro-ISDN (EDSS1):

Ursprung der Meldung:

00:	DEFENDO
01:	lokale Telefonanlage
02:	lokaler Anschluß an das öffentliche Telefonnetz
03:	innerhalb des öffentlichen Telefonnetzes
04:	Anschluß der Gegenstelle an das öffentliche Telefonnetz
05:	Telefonanlage oder Endgerät der Gegenstelle
07:	internationales Telefonnetz

Grund der Meldung:

01:	ungültige MSN – bitte geben Sie die korrekte MSN ein
10:	normaler Verbindungsabbau
11:	Gegenstelle besetzt
12:	An der angerufenen Nummer ist kein Gerät aktiv
15:	Anruf von der Gegenstelle abgewiesen
22:	Kein Kanal mehr frei
2A:	Telefonanlage überlastet

58: Gegenstelle ist inkompatibel (Datenverbindung zu Telefon)

nationales ISDN (1TR6)

Ursprung der Meldung:

44: öffentliches Telefonnetz

45: Telefonanlage oder Endgerät

Grund der Meldung:

00: normaler Verbindungsabbau

08: kein Kanal mehr frei

3A: An der angerufenen Nummer ist kein Gerät aktiv

3B: Gegenstelle besetzt

3E: Anruf von der Gegenstelle abgewiesen

Dies ist nur eine Auswahl der möglichen Meldungen. Weitere Informationen zu den Meldungen erhalten Sie, wenn Sie sich über die Konsole des DEFENDO oder mit Hilfe des telnet-Programmes auf dem DEFENDO als Benutzer admin anmelden. Geben Sie dort den Befehl „man isdn_cause“ ein.

Ursache für andere Meldungen als die zuvor beschriebenen könnten sein:

Falsches D-Kanal-Protokoll (z.B. EDSS1 statt 1TR6)

Falsche oder fehlende Amtsholung

Datenrufe in der Telefonanlage nicht freigeschaltet

Datenrufe werden über einen anderen Telefonprovider abgewickelt (Least-Cost-Router, Preselection), der Datenrufe nicht oder nur eingeschränkt unterstützt.

Absturz einer Komponente der Telefonanlage

11.2.4.4. wichtige Meldungen – nur Intrusion Detection

Die Intrusion Detection untersucht den Inhalt von IP-Paketen anhand einer Signaturdatenbank und meldet verdächtige Pakete über diese Logdatei. Die Einträge im Log enthalten neben Datum, Uhrzeit, Hostname und Prozeß-ID folgende Informationen:

[Modul-ID:SID:Revision] Meldung - URL ...: <Schnittstelle> {Protokoll} Quelle –> Ziel

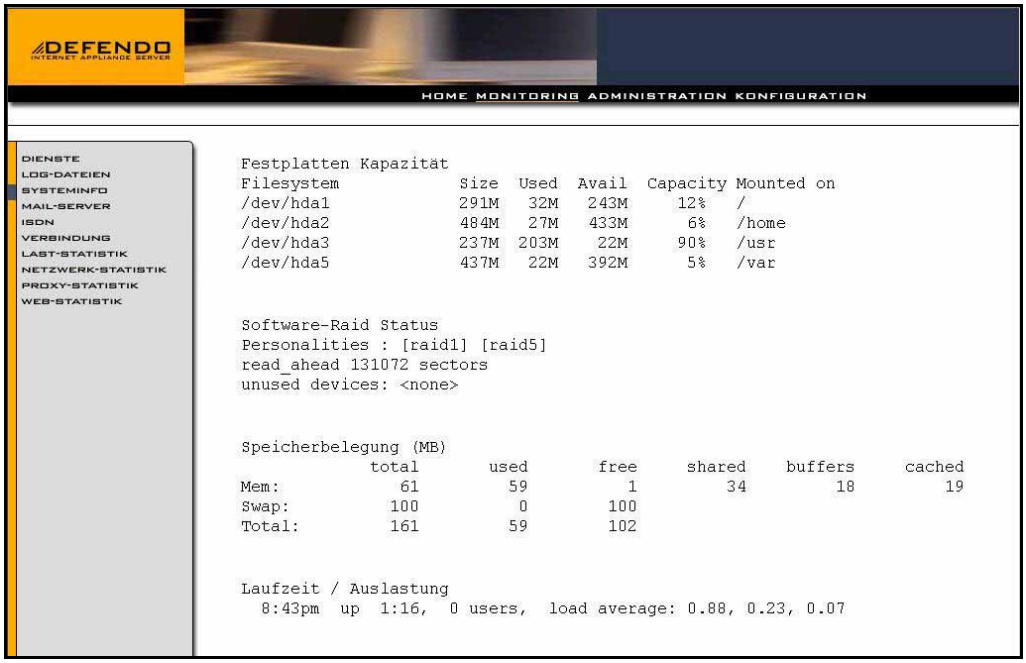
Im folgenden Beispiel wurde an Schnittstelle eth0 ein ICMP-Paket protokolliert, das von der IP-Adresse 169.254.50.3 an 169.254.50.5 gesendet wurde. Gemäß der Meldung handelt es sich um ein (ungewöhnlich) großes ICMP Paket. Nähere Informationen sind unter der angegebenen URL im Internet zu erhalten. Die Signaturkennung (SID) ist 499.

Jul 14 11:40:35 gw snort[22207]: [1:499:1] MISC Large ICMP Packet - http://www.whitehats.com/info/IDS246 [Classification: Potentially Bad Traffic] [Priority: 2]: <eth0> {ICMP} 169.254.50.3 -> 169.254.50.5

11.3. Systeminfo

Hier können Sie u.a. Informationen über den Zustand bzw. die Auslastung der Festplatte des DEFENDO und – sofern vorhanden - der Software-Plattenspiegelung abrufen. Zudem wird angegeben, wie der Hauptspeicher genutzt wird.

Im Bereich „Laufzeit/Auslastung“ stehen weitere Informationen zur Verfügung. Dazu gehört die aktuelle Uhrzeit und die Zeit die seit dem letzten Systemstart vergangen ist. Die Prozessor- bzw. Systemauslastung wird über den Punkt „load average“ angezeigt. Hierbei wird ein Mischwert generiert, der zum Einem angibt, wie stark der Prozessor durch bestimmte Tätigkeiten „ausgebremst“ wird und zum Anderen die Beeinträchtigung der IO-Leistung (z.B. bei vielen Plattenzugriffen). Eine Auslastung von 100% entspricht dem Wert 1.00. Es wird zwischen drei Bereichen unterschieden: Der erste zeigt die Auslastung der letzten Minute an. Beim zweiten ist die Auslastung des Systems in den letzen 5 Minuten ersichtlich. Der dritte dient für die letzten 15 Minuten.



11.4. Mail-Server

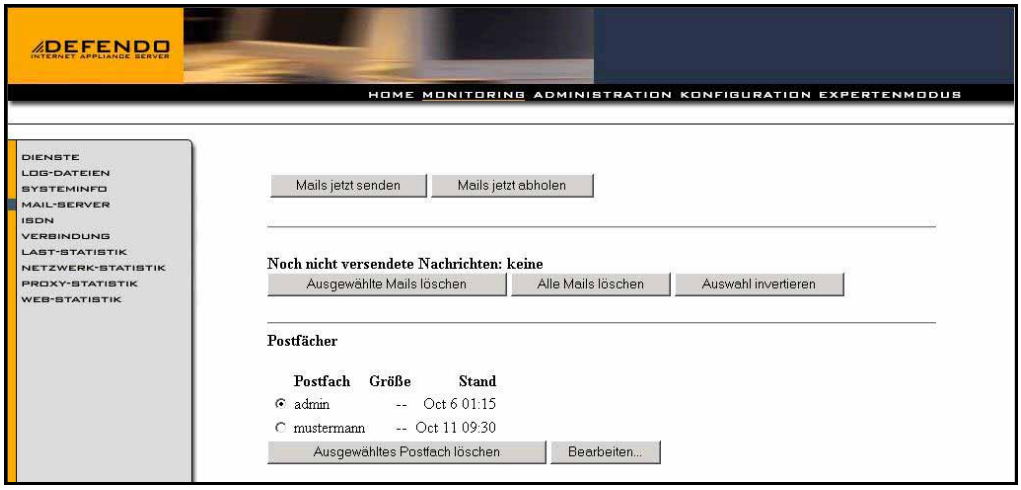
Der Schalter „Mails jetzt senden“ aktiviert den Versand von noch nicht versendeten Mails.

Mit Hilfe des Schalters „Mails jetzt abholen“ können Sie interaktiv die Abholung von Mails aus dem Internet starten. Es öffnet sich ein neues Browser-Fenster in dem der gesamte Prozeß der Mail-Abholung von den Konfigurierten POP3- bzw. ETRN-Servern ersichtlich wird. Insbesondere lassen sich hier auch Fehler bei der Anmeldung am Mail-Server und die Verteilung der Mails bei Sammelpostfächern beobachten.

Mails in der Warteschlange des Mail-Servers werden im Bereich „Noch nicht versendete Nachrichten“ gelistet. Neben der Mail-Server-internen ID sind hier der aktuelle Status der Mail, die Größe in Bytes und der Zeitpunkt zu dem die Mail in die Warteschlange aufgenommen wurde ersichtlich. Es folgen der Absender und der Empfänger der Nachricht.. Bei Problemen wird ferner die zugehörige Fehlermeldung angezeigt.

Um einzelne Mails aus der Warteschlange zu löschen, wählen Sie diese bitte mit Hilfe der Schaltfläche vor der ID aus und drücken Sie dann den Schalter „Ausgewählte Mails löschen“. Der Schalter „Alle Mails löschen“ entfernt entsprechend alle Nachrichten aus der Warteschlange.

Der Schalter „Auswahl invertieren“ erlaubt es Ihnen alle ausgewählten Mails zu deselektieren und alle nicht selektierten Mails auszuwählen.



Es folgt eine Liste der POP3-/IMAP4-Konten des DEFENDO. Neben dem Kontonamen ist die gesamte Größe angegeben. Die folgenden Spalten geben Datum und Uhrzeit des letzten Zugriffs auf dieses Postfach an (letzte eingehende Nachricht oder letzte Leerung des Postfaches). Konten zu Benutzern die zwar angelegt wurden, auf die jedoch noch nie zugegriffen wurde, sind in dieser Übersicht möglicherweise nicht zu sehen.

Ein Mail-Konto wird gelöscht, sobald der zugehörige Benutzer in der Benutzerverwaltung vollständig gelöscht wird. Wird der Benutzer lediglich aus der Gruppe system-mail entfernt, bleibt das Postfach erhalten und kann wieder vom Benutzer genutzt werden sobald er wieder Mitglied der Gruppe system-mail ist.

Mit Hilfe der Schaltflächen vor dem Postfach-Namen kann ein einzelnes Konto ausgewählt werden. Durch Drücken des Schalters „Ausgewähltes Postfach löschen“ wird dieses aus dem System entfernt. Erhält der entsprechende Benutzer zu einem späteren Zeitpunkt wieder eine eMail in sein Postfach, so wird das Postfach automatisch wieder angelegt.

Wählen Sie ein Postfach aus und drücken Sie den Schalter „Bearbeiten“ um den Inhalt des Postfaches zu sehen. Von jeder Nachricht werden hier Absender, Betreff, Größe (sofern verfügbar) und Datum angezeigt. Einzelne Mails können hier nach Selektion gelöscht werden.

11.5. ISDN

Hierbei haben Sie die Möglichkeit, „online“ nachzusehen, ob gerade eine ISDN-Verbindung zum bzw. Vom DEFENDO aus besteht. Für jede ISDN-Karte sind 2 Leitung getrennt zu verfolgen. Die Karten und jeweiligen Kanäle der Karte sind entsprechend nummeriert.

Ist ein Kanal „grün“ gekennzeichnet, so bedeutet dies, dass dieser Kanal der ISDN-Karte frei ist.

Bei einer „gelben“ Zeile wird gerade eine Verbindung aufgebaut.

Eine „rote“ Anzeige mit einer Rufnummer sagt aus, dass über diesen Kanal gerade eine Verbindung besteht.

Im Feld Telefonnummer wird bei ausgehenden Rufen die entsprechende angerufene Nummer angezeigt. Bei eingehenden Rufen erscheint die Nummer des Anrufers oder die 0 wenn dessen Rufnummernübermittlung ausgeschaltet ist.

Sollten Sie eine Standleitung besitzen, so wird ein nicht genutzter Kanal über ein „blaue“ Schriftfarbe angezeigt.

Bitte beachten Sie, daß die Statusanzeige der ISDN-Karte in der Hauptmaske nicht aktualisiert wird. Um eine kontinuierliche Anzeige zu erhalten, drücken Sie bitte auf den entsprechenden Link, der ein neues Fenster öffnet. Die Anzeige in diesem Fenster wird alle 5 Sekunden aktualisiert.

Mit Hilfe der Schalter „Jetzt anwählen“ und „Jetzt auflegen“ können Sie die ausgewählte Schnittstelle dazu veranlassen, die Verbindung zu erstellen bzw. zu trennen. Bitte beachten Sie, dass die Schnittstelle nur wählen kann, wenn eine Rufnummer eingetragen ist und die Schnittstelle aktiviert ist.

Im unteren Teil der Maske können Sie eine Statistik über die Wählverbindung abfragen, über die aktuell die Default-Route gelegt ist. Zudem kann hier eine Überwachung der Online-Zeiten eingestellt werden. Ist die Default-Route nicht über eine PPP-Wählleitung konfiguriert, fehlen diese Einstellmöglichkeiten.

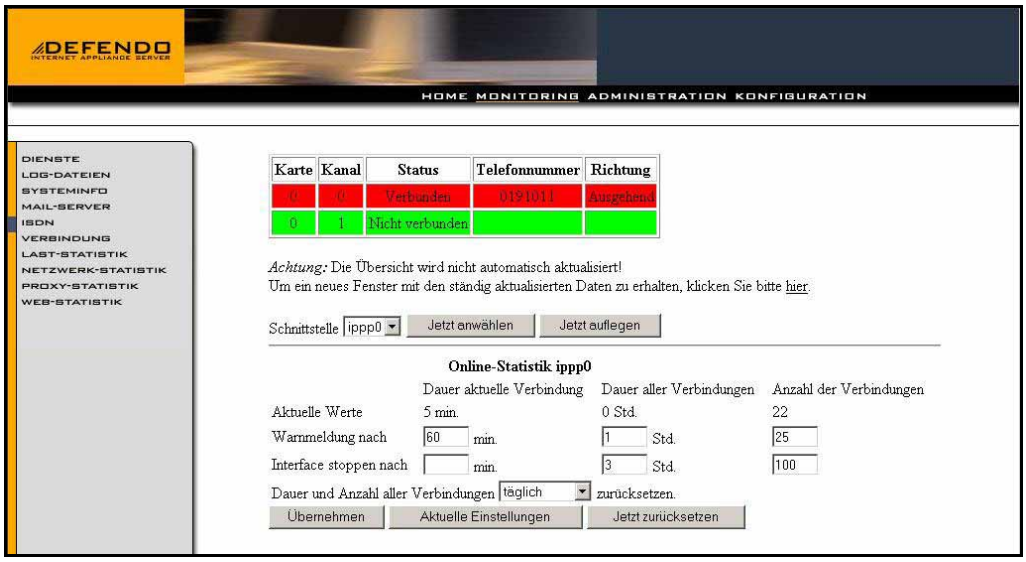
Die Überwachung der Online-Zeiten bezieht sich auf die Dauer einer Verbindung, auf die Dauer aller Verbindungen im angegebenen Intervall und die Anzahl aller Verbindungen im angegebenen Intervall. Für jedes dieser Kriterien kann angegeben werden, wann per Mail eine entspre-

chende Warnmeldung an den admin geschickt werden soll und wann zusätzlich die komplette Schnittstelle deaktiviert werden soll. Tragen Sie den gewünschten Wert in das jeweilige Feld ein bzw. lassen Sie das Feld leer, wenn dieses Kriterium nicht berücksichtigt werden soll. Drücken Sie dann auf Übernehmen um geänderte Einstellungen zu aktivieren.

Sollte eine Schnittstelle aufgrund der Überschreitung deaktiviert worden sein, so ist der zugehörige Dienst neu zu starten (ISDN bei ISDN-Wählverbindungen, ADSL / PPPoverEthernet bei ADSL-Wählverbindungen.

Die Schnittstellenüberwachung ist nur bei PPP-Wählverbindungen möglich (Schnittstellen mit Namen die mit ippp oder adsl beginnen). Ein Verbindungsaufbau wird erst nach erfolgreicher Erstellung der Verbindung auf PPP-Ebene gezählt.

In Ihrem eigenen Interesse empfiehlt es sich, die Überwachung der Einwahldauern zu aktivieren, um sich vor unbeabsichtigt hohen Gebühren zu schützen.


DEFENDO
HOME MONITORING ADMINISTRATION KONFIGURATION
DIENSTE
LOG-DATEIEN
SYSTEMINFO
MAIL-SERVER
ISDN
VERBINDUNG
LAST-STATISTIK
NETZWERK-STATISTIK
PROXY-STATISTIK
WEB-STATISTIK
Karte Kanal Status Telefonnummer Richtung
0 0 Verbunden 0191011 Ausgehend
0 1 Nicht verbunden
Achtung: Die Übersicht wird nicht automatisch aktualisiert!
Um ein neues Fenster mit den ständig aktualisierten Daten zu erhalten, klicken Sie bitte hier.
Schnittstelle ippp0 Jetzt anwählen Jetzt auflegen
Online-Statistik ippp0
Dauer aktuelle Verbindung Dauer aller Verbindungen Anzahl der Verbindungen
Aktuelle Werte 5 min. 0 Std. 22
Warnmeldung nach 60 min. 1 Std. 25
Interface stoppen nach min. 3 Std. 100
Dauer und Anzahl aller Verbindungen täglich zurücksetzen.
Übernehmen Aktuelle Einstellungen Jetzt zurücksetzen

11.6. Verbindung

Hier erhalten Sie die Möglichkeit, bestimmte IP-Adressen zu „pingen“, d. h. nachzusehen, ob diese erreichbar sind. Dies können Adressen im lokalem LAN oder auch Adressen im öffentlichen Internet sein.

Zudem können Anfragen an DNS-Server gemacht werden. Hierbei ist die Wahlmöglichkeit gegeben, über welchen DNS-Server die Anfrage stattfinden soll. Dies kann zum einen der DEFENDO selber sein, oder auch der DNS Ihres Providers. Auch wird standardmäßig der DNS-Server der DENIC vorgegeben. Sollte im Firewallmodul die Option aktiviert sein, daß ausschließlich von den Nameservern des Providers DNS-Antworten akzeptiert werden, so wird eine Anfrage an den DENIC-Server nur dann Erfolg haben, wenn Sie keinen Provider-DNS hinterlegt haben. Über das vorhandene Listenfeld kann eine Auswahl getroffen werden, nach welcher Art von Information Sie im DNS suchen wollen. Zur Auswahl stehen:

A	IP-Adresse zum Namen oder Name zur IP
MX	Mail-Server zur angegebenen Domain
NS	Name-Server zur angegebenen Domain
SOA	Informationen zur angegebenen Domain

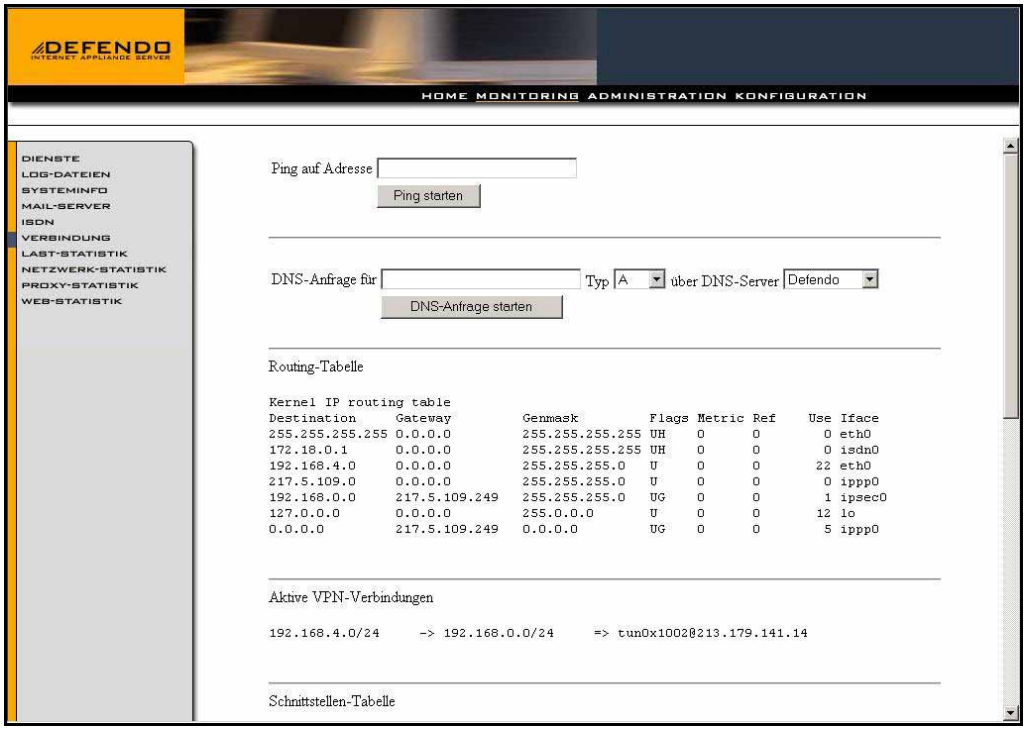
Über die Schalter “Ping starten” und „DNS-Anfrage starten“ können die entsprechenden Funktionen ausgelöst werden.

Im mittleren Teil der Seite sehen Sie die eingerichtete Routing-Tabelle Ihres DEFENDO. Auch ist ersichtlich, von welcher Schnittstelle die Route genützt wird (Iface).

Aktive VPN-Verbindungen

Hier werden alle zur Zeit gültigen VPN Security-Associations angezeigt. Es werden jeweils die Quell- und Zieladressen der zu verschlüsselnden Pakete angegeben. Ferner ist die IP-Adresse des VPN-Servers der Gegenstelle ersichtlich.

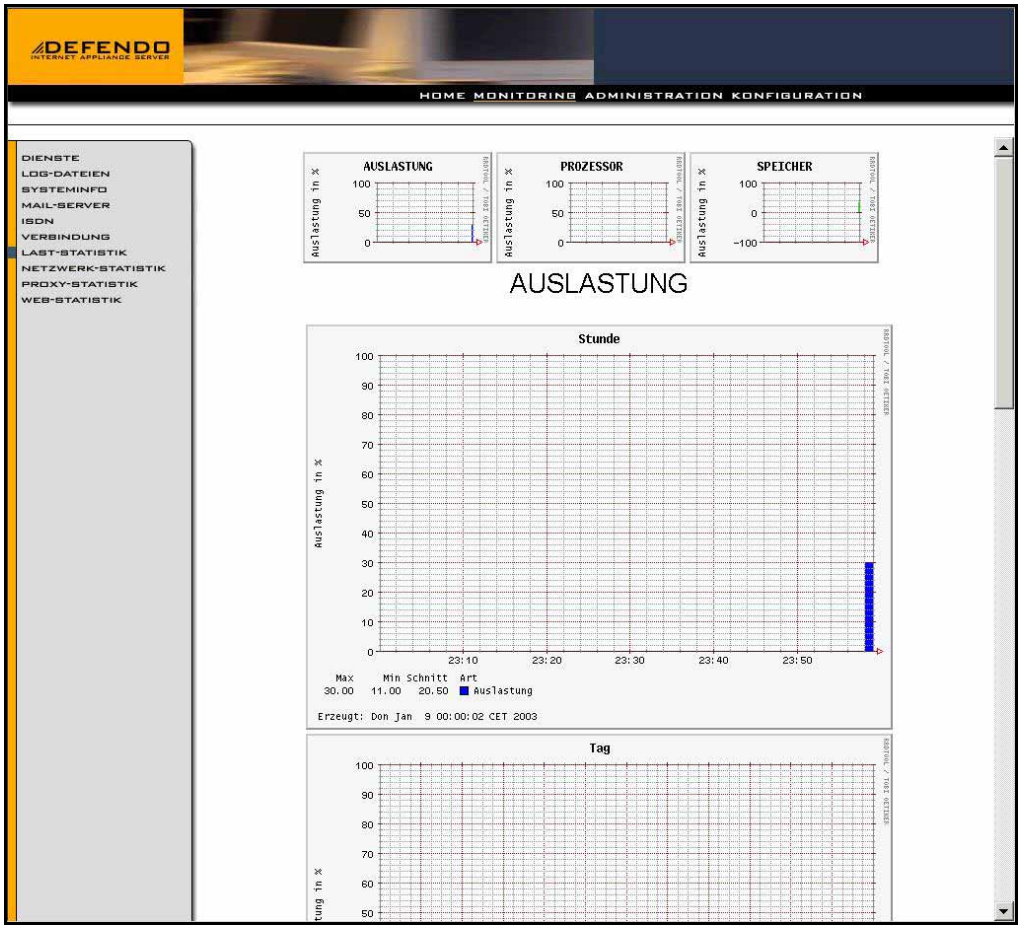
Im unteren Abschnitt der Seite sehen Sie die installierten bzw. aktivierten Schnittstellen Ihres DEFENDO mit deren IP-Adresse und Netzmaske. Je Schnittstelle laufen dabei auch Paketzähler für eingehende (Rx) und ausgehende (Tx) Pakete mit. Ferner werden Probleme in der Schnittstelle ersichtlich (Errors, Carrier).



11.7. Last-Statistik

Unter diesem Menüpunkt erhalten Sie graphische Statistiken über die Auslastung des Systems als Ganzes, die Auslastung des Prozessors sowie über die Speicherbelegung. Die Anzeigen erfolgen jeweils in Prozent.

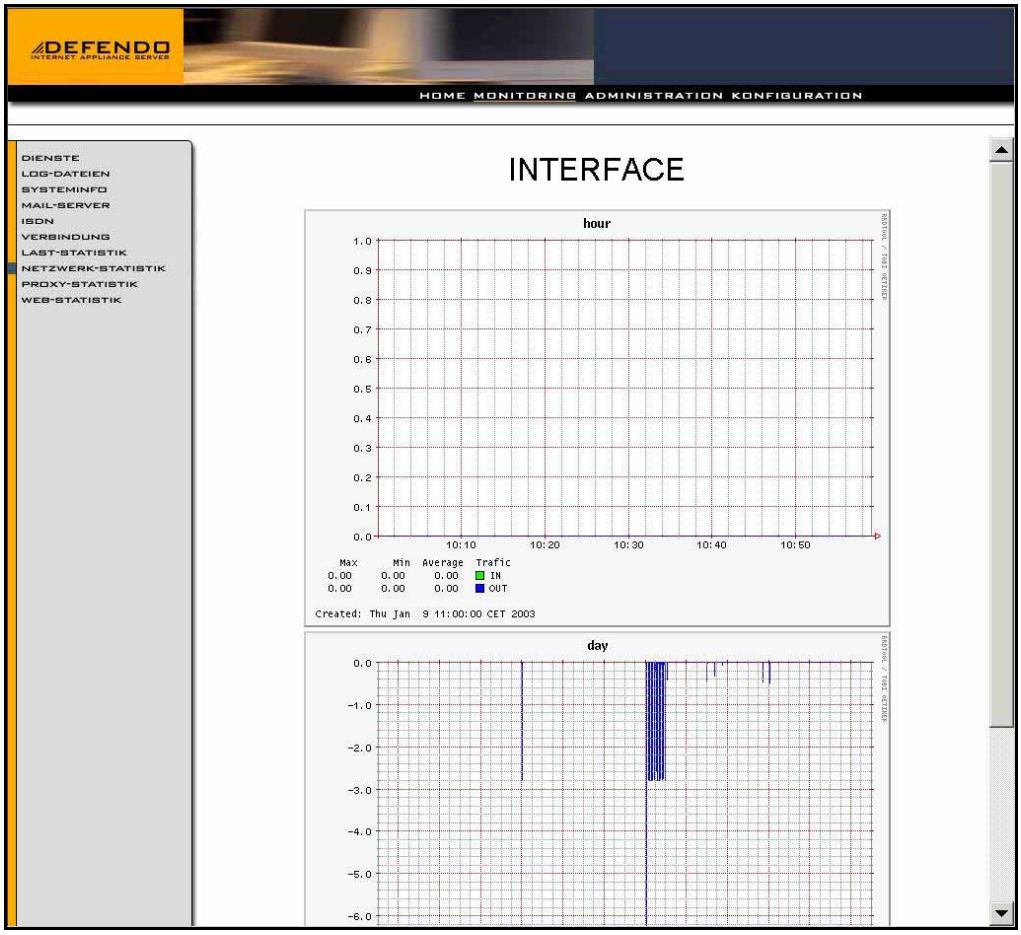
Die wichtigste Statistik ist hier die Auslastungsstatistik. Sie gibt an, wie viele Prozesse im Durchschnitt zur Ausführung bereitstehen. Erreicht dieser Wert 100%, so ist im Durchschnitt zu jedem Zeitpunkt ein Prozeß aktiv. Übersteigt dieser Wert 100%, so müssen Prozesse auf Betriebsmittel warten (Prozessor, Festplattenzugriff, ...).



Die kleinen Graphiken am oberen Bildrand stellen jeweils die letzte Stundenstatistik dar. Sie dienen zugleich als Umschalter zwischen den einzelnen Statistiken. Klicken Sie auf die jeweils gewünschte Graphik, um zwischen den Statistiken zu wechseln. Im unteren Bereich sind zu jeder Statistik jeweils die Stunden-, Tages-, Wochen-, Monats- und Jahres-Statistik zu finden.

11.8. Netzwerk-Statistik

Die Netzwerkstatistik stellt die durchschnittlich übertragene Datenmenge über die Internetschnittstelle dar. Aus dem Internet empfangene Daten werden dabei mit positiven Werten aufgetragen, in das Internet gesendete Daten negativ. Die Anzeige erfolgt in kByte pro Zeiteinheit. Es stehen eine Stunden-, Tages-, Wochen-, Monats- und Jahres-Statistik zur Verfügung.

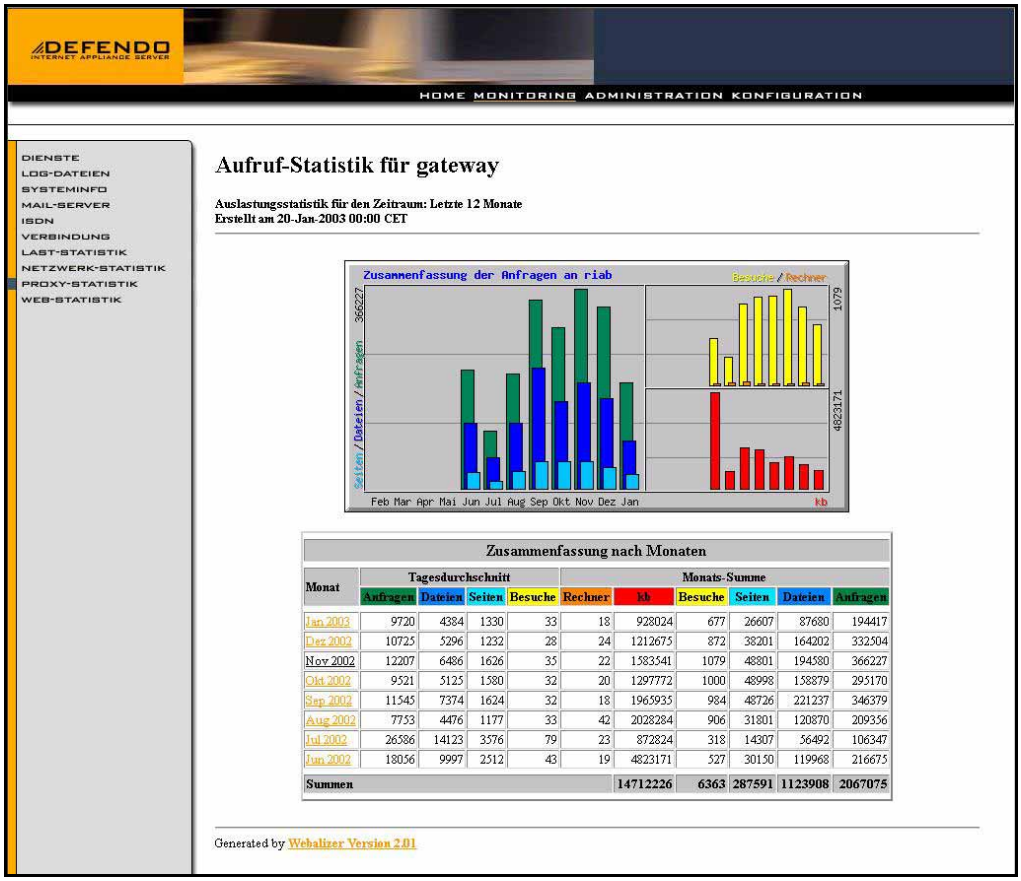


11.9. Proxy-Statistik

Der Menüpunkt Proxystatistik bietet Ihnen einen Einblick, in das „Surf"-Verhalten Ihrer Mitarbeiter. Hierbei wird eine „Online-Statistik" geführt, die protokolliert wann, wohin und wieviel gesurft wurde. Auch die IP-Adresse des PCs der gesurft hat wird protokolliert. Ist die Benutzeranmeldung im Proxy-Cache aktiviert, so erhalten Sie ferner eine Summe der vom jeweiligen Benutzer in Anspruch genommenen Datenmenge.

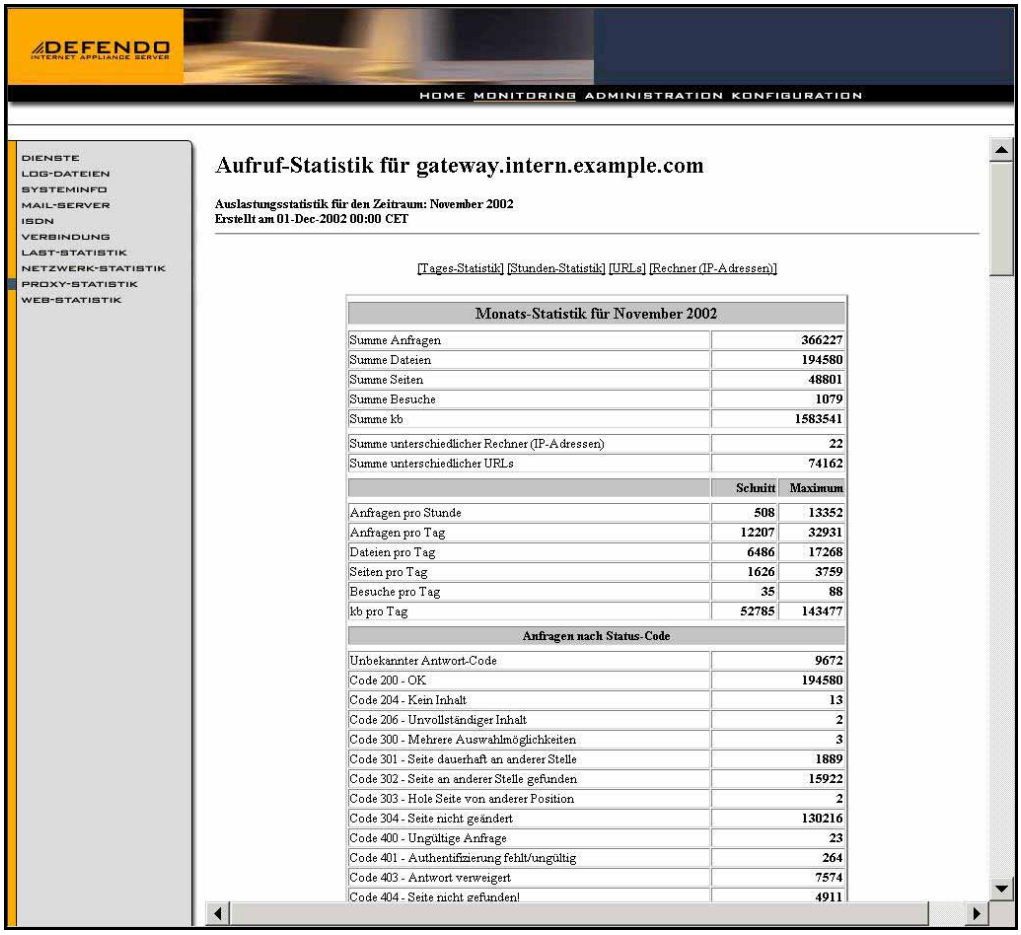
> *Hinweis:*
>
> *Ist im Proxy-Cache der Virenscan bzw. Tagfilter aktiviert, ist eine Auswertung nach der IP-Adresse des PC der gesurft hat nicht möglich.*

Die Statistik wird täglich einmal im Nachtlauf aktualisiert.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
DIENSTE
LOG-DATEIEN
SYSTEMINFO
MAIL-SERVER
ISDN
VERBINDUNG
LAST-STATISTIK
NETZWERK-STATISTIK
PROXY-STATISTIK
WEB-STATISTIK
Aufruf-Statistik für gateway
Auslastungsstatistik für den Zeitraum: Letzte 12 Monate
Erstellt am 20-Jan-2003 00:00 CET
Zusammenfassung der Anfragen an riab
Besuche / Rechner
366227
Seiten / Dateien / Anfragen
1079
4823171
Feb Mar Apr Mai Jun Jul Aug Sep Okt Nov Dez Jan
kb
Zusammenfassung nach Monaten
Monat
Tagesdurchschnitt
Monats-Summe
Anfragen Dateien Seiten Besuche Rechner kb Besuche Seiten Dateien Anfragen
Jan 2003 9720 4384 1330 33 18 928024 677 26607 87680 194417
Dez 2002 10725 5296 1232 28 24 1212675 872 38201 164202 332504
Nov 2002 12207 6486 1626 35 22 1583541 1079 48801 194580 366227
Okt 2002 9521 5125 1580 32 20 1297772 1000 48998 158879 295170
Sep 2002 11545 7374 1624 32 18 1965935 984 48726 221237 346379
Aug 2002 7753 4476 1177 33 42 2028284 906 31801 120870 209356
Jul 2002 26586 14123 3576 79 23 872824 318 14307 56492 106347
Jun 2002 18056 9997 2512 43 19 4823171 527 30150 119968 216675
Summen 14712226 6363 287591 1123908 2067075
Generated by Webalizer Version 2.01

Der Verlauf verschiedener Größen während der letzten 12 Monate ist hier sowohl graphisch als auch tabellarisch mit den entsprechenden Zahlenwerten aufgetragen.

Wollen Sie einen Monat genauer auswerten, so klicken Sie diesen in der Monatsstatistik an. Hierunter werden die einzelnen Monate spezifischer ausgewertet. Alle Angaben sind über farbliche Agenden erklärt.

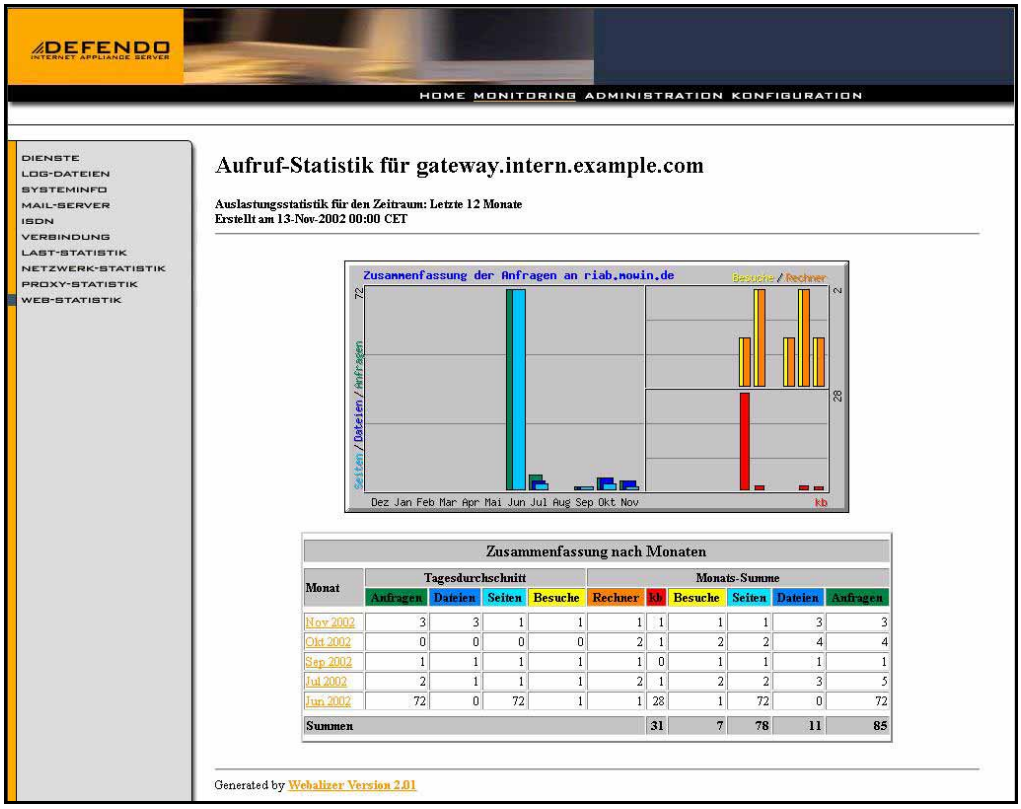

DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
DIENSTE
LOG-DATEIEN
SYSTEMINFO
MAIL-SERVER
ISDN
VERBINDUNG
LAST-STATISTIK
NETZWERK-STATISTIK
PROXY-STATISTIK
WEB-STATISTIK
Aufruf-Statistik für gateway.intern.example.com
Auslastungsstatistik für den Zeitraum: November 2002
Erstellt am 01-Dec-2002 00:00 CET
[Tages-Statistik] [Stunden-Statistik] [URLs] [Rechner (IP-Adressen)]
Monats-Statistik für November 2002
Summe Anfragen 366227
Summe Dateien 194580
Summe Seiten 48801
Summe Besuche 1079
Summe kb 1583541
Summe unterschiedlicher Rechner (IP-Adressen) 22
Summe unterschiedlicher URLs 74162
Schnitt Maximum
Anfragen pro Stunde 508 13352
Anfragen pro Tag 12207 32931
Dateien pro Tag 6486 17268
Seiten pro Tag 1626 3759
Besuche pro Tag 35 88
kb pro Tag 52785 143477
Anfragen nach Status-Code
Unbekannter Antwort-Code 9672
Code 200 - OK 194580
Code 204 - Kein Inhalt 13
Code 206 - Unvollständiger Inhalt 2
Code 300 - Mehrere Auswahlmöglichkeiten 3
Code 301 - Seite dauerhaft an anderer Stelle 1889
Code 302 - Seite an anderer Stelle gefunden 15922
Code 303 - Hole Seite von anderer Position 2
Code 304 - Seite nicht geändert 130216
Code 400 - Ungültige Anfrage 23
Code 401 - Authentifizierung fehlt/ungültig 264
Code 403 - Antwort verweigert 7574
Code 404 - Seite nicht gefunden! 4911

11.10. Web-Statistik

Sollte Ihr DEFENDO zugleich als Internet-Web-Server fungieren, so ist dieser Menüpunkt Ihnen sicherlich sehr hilfreich. Mit ihm können Sie ersehen, welche Zugriffe Ihr Web-Server hatte, woher diese Zugriffe stammen, welche Seiten eingesehen wurden und auf welche Dateien ein Zugriff stattfand.

Auch in diesem Bereich sind alle Angaben mit farblichen Agenden versehen, die Ihnen ein Zurechtfinden sehr einfach machen.

Die Statistik wird täglich einmal über Nacht aktualisiert.


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION
DIENSTE
LOG-DATEIEN
SYSTEMINFO
MAIL-SERVER
ISDN
VERBINDUNG
LAST-STATISTIK
NETZWERK-STATISTIK
PROXY-STATISTIK
WEB-STATISTIK
Aufruf-Statistik für gateway.intern.example.com
Auslastungsstatistik für den Zeitraum: Letzte 12 Monate
Erstellt am 13-Nov-2002 00:00 CET
Zusammenfassung der Anfragen an riab.mowin.de
Besuche / Rechner
Seiten / Dateien / Anfragen
72
28
2
Dez Jan Feb Mar Apr Mai Jun Jul Aug Sep Okt Nov
kb
Zusammenfassung nach Monaten
Monat
Tagesdurchschnitt
Monats-Summe
Anfragen
Dateien
Seiten
Besuche
Rechner
kb
Besuche
Seiten
Dateien
Anfragen
Nov 2002 3 3 1 1 1 1 1 1 3 3
Okt 2002 0 0 0 0 2 1 2 2 4 4
Sep 2002 1 1 1 1 1 0 1 1 1 1
Jul 2002 2 1 1 1 2 1 2 2 3 5
Jun 2002 72 0 72 1 1 28 1 72 0 72
Summen 31 7 78 11 85
Generated by Webalizer Version 2.01

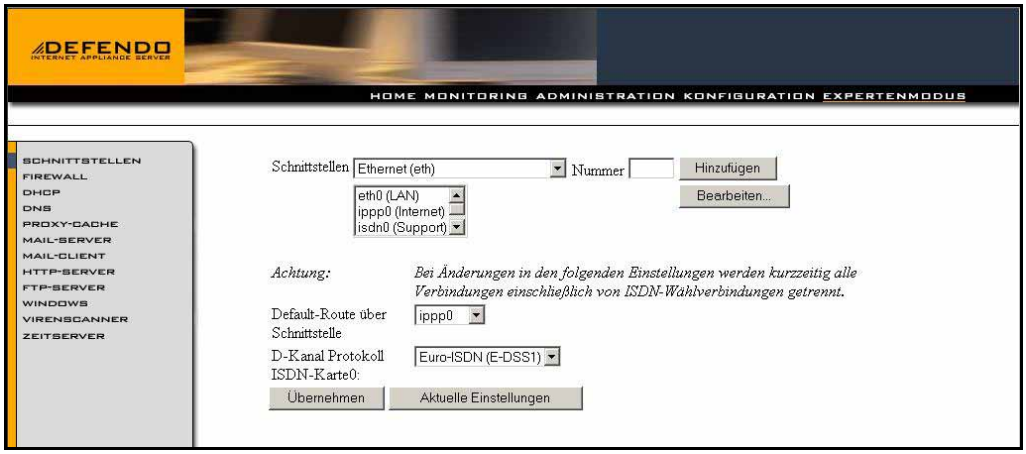
12. Das Hauptmenü „Expertenmodus“

Die meisten Dinge, die bereits über die Konfigurations-Assistenten eingestellt wurden, finden Sie hier wieder, jedoch in Form von „Modulen“. Somit sind Sie jederzeit in der Lage, spezifische Änderungen vorzunehmen, Auch spezielle Einstellungen wie z. B. der Firewall können hier getätigt werden. Generell ist unter diesem Menüpunkt zu beachten, dass ein entsprechendes IT-Fachwissen vorausgesetzt werden muss, da einige Einstellungen dazu führen können, dass Ihr System nicht mehr sicher ist bzw. instabil laufen kann. Zudem könnten Sie sich von der Administration des DEFENDO aussperren.

Ist der Menüpunkt „Expertenmodus“ im Hauptmenü nicht zu sehen, so muß dieser erst über den entsprechenden Menüpunkt aus dem Bereich „Konfiguration“ freigegeben werden.

12.1. Schnittstellen

Über den Menüpunkt Schnittstellen sind Sie in der Lage, bestehende Kommunikationsschnittstellen des DEFENDO zu bearbeiten oder hinzuzufügen. Auch wird hier angegeben, über welche Schnittstelle die Default-Route in das Internet gelegt werden soll.



Um eine neue Schnittstelle anzulegen, wählen Sie hier bitte den Schnittstellentyp aus. Geben Sie dann in das Feld Nummer die Ziffer der Schnittstelle ein, die Sie anlegen wollen. Bitte beachten Sie, daß jede Ziffer nur einmal vorhanden sein darf und je nach Schnittstellentyp bestimmten Beschränkungen unterliegt. Drücken Sie auf Hinzufügen um die neue Schnittstelle anzulegen.

Wählen Sie eine Schnittstelle aus der Liste aus und drücken Sie auf Bearbeiten um Einstellungen der Schnittstelle zu verändern oder die Schnittstelle zu löschen.

- Ethernet (eth): Ethernet Schnittstelle werden außer zur Anbindung des LANs für die Verbindung mit externen Routern und zur Einrichtung einer Demilitarisierten Zone (DMZ) benötigt. Die Ziffer wird fortlaufend von 0 an vergeben und wird durch die Reihenfolge in der die Netzwerkkarten-Treiber geladen werden den physikalisch eingebauten Netzwerkkarten zugeordnet. Bitte beachten Sie, daß die Treiber für neu eingebaute Netzwerkkarten von Ihrem DEFENDO-Support (siehe Kapitel 14)eingetragen werden müssen.
- ISDN syncPPP (ippp): ISDN-PPP Schnittstelle. Üblicherweise erfolgt die Anbindung an den Provider per ISDN-Wählleitung über das PPP-Protokoll. Ein weiterer Anwendungspunkt ist die RAS-Einwahl für Außenstellen oder Mitarbeiter. Die Schnittstellen-Nummer ist aus dem Bereich 0 bis 62 zu vergeben. Auch bei ISDN-Standleitungen findet dieser Schnittstellentyp Verwendung.
- ISDN HDLC-RawIP (isdn): Über ISDN Schnittstellen dieses Typs ist keine Benutzeranmeldung möglich. Bei erforderlicher Benutzeranmeldung verwenden Sie bitte PPP-Schnittstellen.

HDLC-RawIP wird häufig bei ISDN-Standleitungen verwendet. Die Schnittstellen-Nummer ist frei zu vergeben.

- ADSL / PPP over Ethernet (adsl): Sollten Sie eine ADSL-Wählleitung anbinden wollen, so benötigen Sie diesen Schnittstellen-Typ. Die Schnittstellen-Nummer ist frei zu vergeben. Bitte beachten Sie, daß die Anbindung einer ADSL-Standleitung über einen externen Router mit Ethernet-Schnittstelle erfolgt. Sie benötigen für ADSL-Standleitungen also eine Ethernet-Schnittstelle.
- Serielles Modem (ttyS): Für die analoge RAS-Einwahl mit Hilfe eines seriellen Modems wird diese Schnittstelle benötigt. Die Schnittstellen-Nummer entspricht dabei dem verwendeten seriellen Port (0 für COM1, 1 für COM2, usw.). Bitte beachten Sie, daß eine analoge Einwahl bei Ihrem Internet-Provider über diese Schnittstellenart nicht möglich ist.
- VPN (ipsec): Mit Hilfe dieses Schnittstellentyps wird läßt sich ein Virtual-Privat-Network (VPN) konfigurieren. Als Schnittstellen-Nummer ist eine Zahl zwischen 0 und 3 zulässig. Soll VPN auf eine Schnittstelle mit dynamischer IP-Adresse aufgesetzt werden, so darf lediglich die 0 als Schnittstellen-Nummer verwendet werden. Weitere ipsec-Schnittstellen sind dann nicht verfügbar.

Default-Route über Schnittstelle

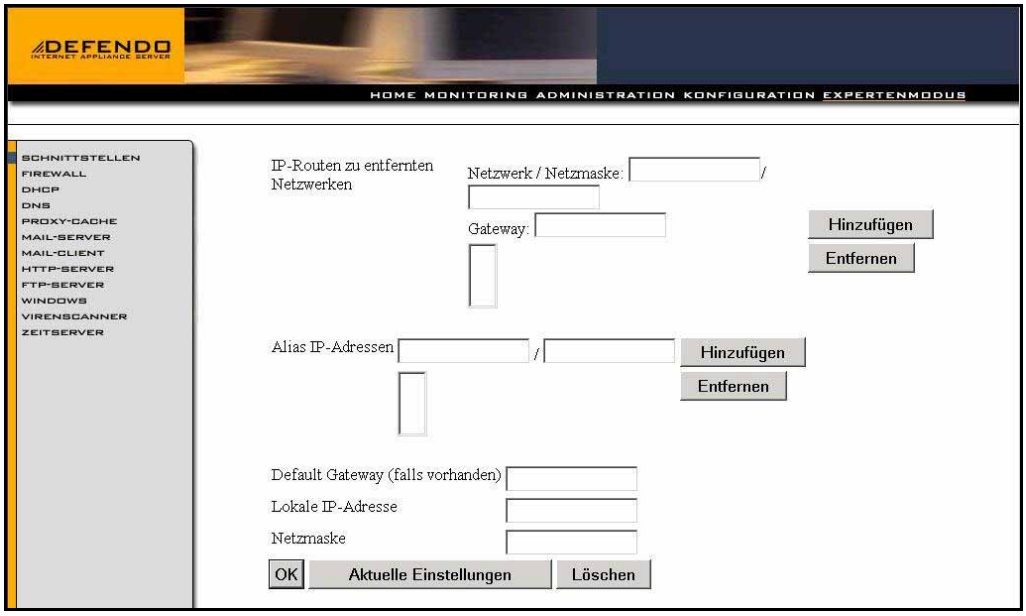
Geben Sie hier die Schnittstelle an, über die die Anbindung an das Internet erfolgt. Alle IP-Pakete mit Zieladressen, für die keine andere Routing-Information vorhanden ist, werden über die hier ausgewählte Schnittstelle versendet. Sie könne diese Einstellung verwenden, um schnell zwischen zwei Internet-Anbindungen zu wechseln (z.B. Standleitung über eth1, ISDN-Wählleitung über ippp0). Bitte beachten Sie jedoch, daß beim Wechsel der Anbindung ggf. auch andere Werte wie verwendete DNS-Server, Proxy-Cache des Providers oder Mail-Relay des Providers an den entsprechenden Stellen zu ändern sind.

D-Kanal Protokoll ISDN-Karte x

Weisen Sie hier den im System eingebauten ISDN-Karten das entsprechende D-Kanal Protokoll zu: Euro-ISDN (E-DSS1) findet Verwendung beim direkten Anschluß an das öffentliche Telefonnetz und beim Anschluß an viele Telefonanlagen. Bei manchen Telefonanlagen findet hingegen das 1TR6-Protokoll Verwendung. Bitte konsultieren Sie dazu den Betreuer Ihrer Telefonanlage. Für das amerikanisch NI1 Protokoll oder beim Betrieb an einer Standleitung wählen Sie bitte den entsprechenden Eintrag.

Drücken Sie auf Übernehmen um die vorgenommenen Änderungen zu aktivieren.

12.1.1. Ethernet



IP-Routen zu entfernten Netzwerken

Sind an das Netzwerk der aktuellen Ethernet-Karte weitere Netzwerke über einen Router angeschlossen, so können Sie hier die erforderlichen Routen zur Kommunikation mit diesen Netzwerken einrichten. Tragen Sie die Netzwerkadresse und die zugehörige Netzmaske des indirekt angeschlossenen Netzes ein. Als Gateway ist die IP-Adresse des Routers anzugeben. Drücken Sie dann auf Hinzufügen um die Route einzutragen. Sie geben auf diese Weise der Firewall bekannt, daß dieses Netzwerk über die Netzwerkkarte akzeptiert werden muß.

Konfigurierte Routen werden in folgendem Format angezeigt:

Netzwerkadresse/Netzmaske->Gateway

Um eine Route zu löschen, wählen Sie diese aus der Liste aus und drücken Sie auf Entfernen.

Alias IP-Adressen

Nutzen Sie diesen Bereich um der gewählten Ethernet-Karte zusätzliche IP-Adressen zu geben. Es kann sich hierbei um Adressen aus dem gleichen Netzwerk handeln, aus dem auch die primäre IP-Adresse

stammt. Nutzen Sie dies, um z.B. mehrere Internet-Adressen auf die Internet-Schnittstelle zu binden, um anschließend mit Hilfe von Firewall-Regeln (Portforwarding/DNAT) die Zugriffe je angesprochener Adresse auf interne Adressen weiterzuleiten. Möglich ist aber auch die Vergabe von Adressen aus anderen Netzwerken, wenn im selben physikalischen Ethernet-Segment mehrere IP-Netwerke konfiguriert sind.

Tragen Sie die gewünschte zusätzliche IP-Adresse des DEFENDO zusammen mit der zugehörigen Netzmaske in die entsprechenden Felder ein und drücken Sie auf „Hinzufügen“ um die zusätzliche IP-Adresse zu aktivieren. Wählen Sie eine Adresse aus und drücken Sie auf „Entfernen“ damit diese Adresse nicht mehr vom DEFENDO verwendet wird.

Default Gateway (falls vorhanden)

Tragen Sie hier die IP-Adresse des Default-Gateways ein, falls über die aktuell bearbeitete Schnittstelle ein solches erreichbar ist. Ist in der Schnittstellen-Hauptmaske das Default-Gateway auf die aktuell bearbeitete Schnittstelle gestellt, so wird die hier angegebene Adresse als Gateway-Adresse verwendet.

Lokale IP-Adresse

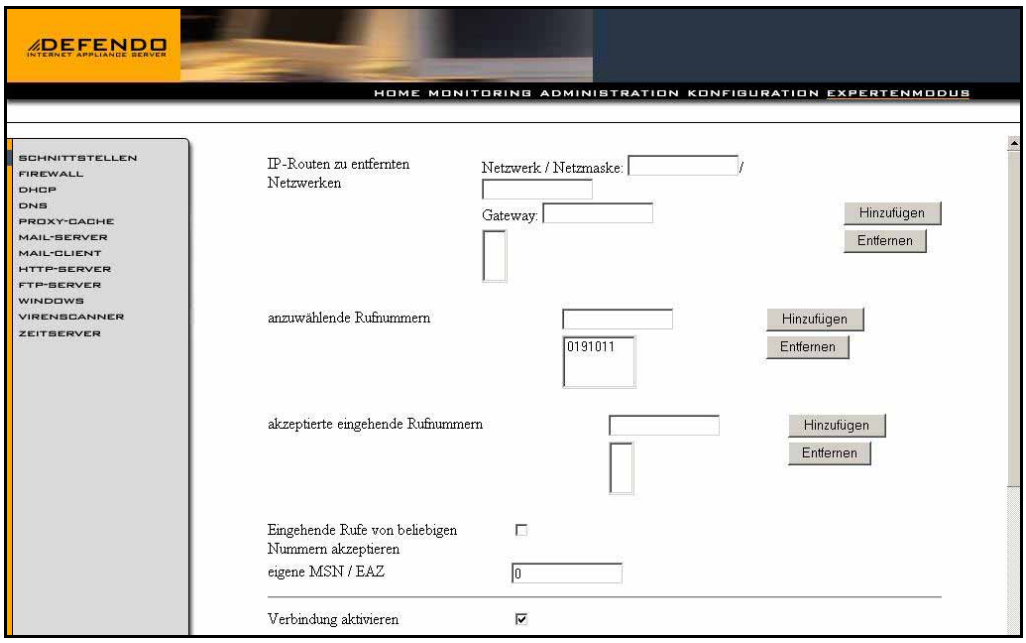
Geben Sie hier die IP-Adresse ein, die der DEFENDO auf der aktuell bearbeiteten Schnittstelle erhalten soll. Bei der Schnittstelle eth0 läßt sich dieser Wert nur mit Hilfe des Menüpunktes Administration->Grundeinstellungen verändern.

Netzmaske

Geben Sie hier die Netzmaske ein, die für das Netzwerk gilt, an das die aktuell bearbeitete Schnittstelle angeschlossen ist. Bei der Schnittstelle eth0 läßt sich dieser Wert nur mit Hilfe des Menüpunktes Administration->Grundeinstellungen verändern.

Drücken Sie auf OK um Änderungen zu aktivieren oder auf Löschen um die gesamte Schnittstelle zu entfernen.

12.1.2. ISDN syncPPP



IP-Routen zu entfernten Netzwerken

Sind über die ISDN-Verbindung weitere Netzwerke angeschlossen, so können Sie hier die erforderlichen Routen zur Kommunikation mit diesen Netzwerken einrichten. Tragen Sie die Netzwerkadresse und die zugehörige Netzmaske des indirekt angeschlossenen Netzes ein. Bei festen IP-Adressen ist als Gateway die IP-Adresse des ISDN-Routers der Gegenstelle anzugeben. Bei dynamischer Adressvergabe geben Sie hier bitte die Adresse 0.0.0.0 ein. Drücken Sie dann auf Hinzufügen um die Route einzutragen. Sie geben auf diese Weise auch der Firewall bekannt, daß dieses Netzwerk über diese ISDN-Schnittstelle akzeptiert werden muß.

Konfigurierte Routen werden in folgendem Format angezeigt:

Netzwerkadresse/*Netzmaske*->*Gateway*

Um eine Route zu löschen, wählen Sie diese aus der Liste aus und drücken Sie auf Entfernen.

Anzuwählende Rufnummern

Geben Sie hier die Rufnummer ein, die angerufen werden soll. Beim Anschluß über eine Telefonanlage ist ggf. die Nummer der Amtsholung voranzustellen. Ist keine Rufnummer angegeben, so sind keine ausgehenden Rufe über diese Schnittstelle möglich.

Akzeptierte eingehende Rufnummern

Tragen Sie hier die Liste der Rufnummern ein, von denen eingehende Anrufe akzeptiert werden sollen. Bei Anrufern die das ISDN-Merkmal der Rufnummernübermittlung ausgeschaltet haben, wird als eingehende Rufnummer die 0 übermittelt.

Eingehende Anrufe von beliebigen Rufnummern akzeptieren

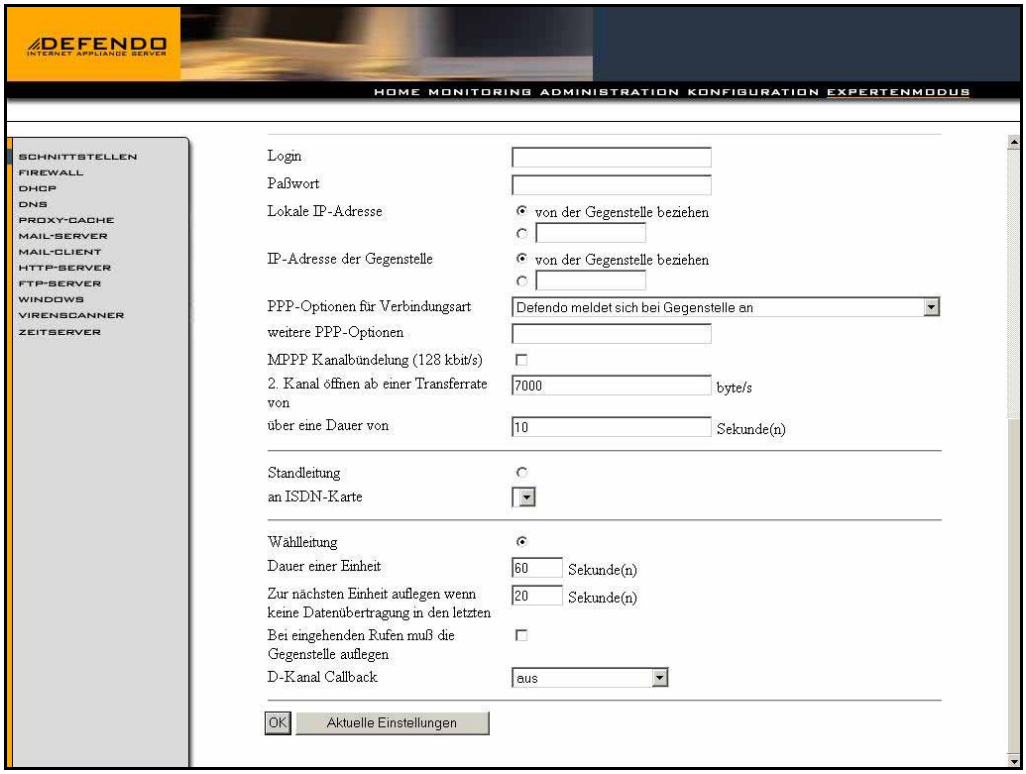
Wenn dieser Schalter aktiviert ist, werden alle eingehenden Anrufe von dieser Schnittstelle akzeptiert. Die Liste der akzeptierten eingehenden Rufnummern ist für diese Schnittstelle außer Kraft gesetzt. Sollten noch weitere Schnittstellen auf die gleiche MSN konfiguriert sein, ist nicht definiert, welche Schnittstelle den Anruf annimmt. Dies kann insbesondere zu Problemen bei der Fernwartung führen. Bitte verwenden Sie daher eine eigene MSN für Schnittstellen mit Rufnummern-Identifizierung sobald Sie auf einer Schnittstelle (egal ob ippp oder isdn) Anrufe von beliebigen Nummern akzeptieren.

Eigene MSN / EAZ

Geben Sie hier bitte die MSN bei Euro-ISDN bzw. die EAZ bei 1TR6 ein. Für das amerikanische NI1 Protokoll geben Sie bitte die MSN und den SPID im Format MSN:SPID an. Beim direkten Anschluß an einen NTBA der Telekom ist die MSN die komplette Rufnummer ohne Ortsvorwahl. Beim Anschluß an eine Telefonanlage ist die MSN häufig identisch mit der Durchwahl. Beim 1TR6-Protokoll darf hier nur genau eine Ziffer eingetragen werden, die im allgemeinen nichts mit der Durchwahl zu tun hat.

Verbindung aktivieren

Ist dieser Schalter deaktiviert, so werden eingehende und ausgehende Verbindungen über diese Schnittstelle unterbunden.



Login:

Geben Sie hier die Benutzerkennung ein, mit der sich der DEFENDO bei der Gegenstelle anmelden soll. Dieses Feld wird nicht benötigt, wenn sich ein Einwähler anmelden soll.

Paßwort

Geben Sie hier das Paßwort ein, mit dem sich der DEFENDO bei der Gegenstelle anmelden soll. Dieses Feld wird nicht benötigt, wenn sich ein Einwähler anmelden soll.

Lokale IP-Adresse

Wählen Sie von der Gegenstelle beziehen, wenn der DEFENDO die IP-Adresse von der Gegenstelle dynamisch zugewiesen bekommen soll. Wenn Sie die lokale IP-Adresse festlegen wollen, setzen Sie bitte den Haken vor dem Eingabefeld und tragen Sie die IP-Adresse des DEFENDO ein. Die IP-Adresse sollte insbesondere bei Einwahl-Schnittstellen (RAS) festgelegt werden um Manipulation und Mißbrauch vorzubeugen.

IP-Adresse der Gegenstelle

Wählen Sie von der Gegenstelle beziehen, wenn der DEFENDO die IP-Adresse der Gegenstelle dynamisch zugewiesen bekommen soll. Wenn der DEFENDO hingegen der Gegenstelle die IP-Adresse zuweisen soll

oder die IP-Adresse der Gegenstelle fest definiert ist, setzen Sie bitte den Haken vor dem Eingabefeld und tragen Sie die IP-Adresse der Gegenstelle ein. Die IP-Adresse sollte insbesondere bei Einwahl-Schnittstellen (RAS) festgelegt werden um Manipulation und Mißbrauch vorzubeugen.

PPP-Optionen für Verbindungsart

Mit Hilfe dieser Auswahlliste können Sie einen Satz von typischen PPP-Optionen für den jeweiligen Anwendungsfall auswählen.

DEFENDO meldet sich bei Gegenstelle an: Wünscht die Gegenstelle eine Anmeldung über PAP oder CHAP, so übermittelt der DEFENDO die unter Login und Paßwort eingegebenen Anmeldedaten. Typischer Anwendungsfall ist die Einwahl bei Ihrem Internet-Service-Provider.

Gegenstelle meldet sich bei DEFENDO an: In diesem Falle besteht DEFENDO darauf, daß sich die Gegenstelle mit PAP authentifiziert. Typischer Anwendungsfall ist die Einwahl einer Außenstelle mit eigenem Router.

Gegenstelle meldet sich bei DEFENDO an und wird Teilnehmer im LAN: Diese Option entspricht der vorhergehenden. Es wird jedoch zusätzlich versucht, den Einwähler mit Hilfe von Proxyarp-Routing transparent in das lokale Netzwerk einzubinden. Typischer Anwendungsfall ist die Einwahl eines einzelnen PCs. Die IP-Adresse die dem Einwähler zugewiesen wird muß dabei eine freie IP-Adresse aus einem anderen am DEFENDO direkt angeschlossenen Netzwerk sein in das der Einwähler eingebunden werden soll.

Ohne Anmeldung: Bei dieser Option meldet sich weder der DEFENDO bei der Gegenstelle an noch wird von der Gegenstelle eine Anmeldung aktzeptiert. Typischer Anwendungsfall ist eine Standleitung mit PPP-Protokoll.

Benutzerdefiniert: Diese Option ist für spezielle Fälle vorgesehen und ausschließlich zur Konfiguration durch den Support gedacht.

Weitere PPP-Optionen

Je nach Gegenstelle sind in seltenen Fällen zusätzliche Optionen notwendig (z.B. das Deaktivieren bestimmter Kompressionsverfahren). Diese Optionen können hier angegeben werden. Dieses Feld ist in erster Linie für den Support gedacht.

MPPP Kanalbündelung 128 kbit/s

Mit diesem Schalter aktivieren Sie die Kanalbündelung mit Hilfe des MPPP-Protokolles. Diese Option ist ausschließlich bei der Schnittstelle

ippp0 verfügbar und muß auch von Seiten des Providers unterstützt werden. Bei der Kanalbündelung wird der zweite ISDN-Kanal der ISDN-Karte bei entsprechend hoher Datentransferrate dynamisch zugeschaltet. Bitte beachten Sie, daß damit zwei ISDN-Leitungen belegt werden und damit auch die Telefongebühren für zwei Leitungen anfallen. Im allgemeinen verlangt auch der Provider zusätzliche Gebühren für den zweiten Kanal. Demgegenüber steht die doppelte Bandbreite zum Provider.

2. Kanal öffnen ab einer Transferrate von ... über eine Dauer von ...

Geben Sie hier die Transferrate in byte pro Sekunde und die Dauer in Sekunden ein für die diese Transferrate mindestens anliegen muß. Werden diese Werte überschritten, wird der 2. Kanal bei aktiver Kanalbündelung aufgeschaltet. Werden die Werte unterschritten, wird der 2. Kanal entsprechend der Einstellungen für den 1. Kanal wieder aufgelegt. Diese Optionen sind ausschließlich bei der Schnittstelle ippp0 verfügbar.

Standleitung an ISDN-Karte

Aktivieren Sie den Haken bei Standleitung und wählen Sie die zugehörige ISDN-Karte aus, wenn diese Schnittstelle an eine Standleitung angeschlossen ist.

Wählleitung

Aktivieren Sie den Haken bei Wählleitung wenn diese Schnittstelle nicht an eine Standleitung angeschlossen werden soll.

Dauer einer Einheit

Zur Optimierung der Verbindungstrennung tragen Sie hier bitte die Dauer einer Gebühreneinheit ein.

Zur nächsten Einheit auflegen wenn keine Datenübertragung in den letzten ... Sekunden

Werden in der hier eingegebenen Zeitspanne vor Ablauf der nächsten Gebühreneinheit keine Daten mehr übertragen, wird die Verbindung automatisch getrennt.

Bei eingehenden Rufen muß die Gegenstelle auflegen

Diese Einstellung ist insbesondere bei RAS-Einwahlverbindungen sinnvoll. Bei eingehenden Rufen (also wenn der Anrufer die Gebühren zahlt) trennt DEFENDO die Verbindung nicht, auch wenn keine Daten mehr über diese Verbindung fließen.

D-Kanal Callback

Sollten Sie die Wählleitung im D-Kanal Callback Verfahren betreiben wollen, so wählen Sie hier bitte die gewünschte Richtung aus. Bei der Auswahl von „Gegenstelle ruft zurück“ erwartet DEFENDO einen Rückruf, wenn der eigene Ruf von der Gegenstelle abgewiesen wurde. Ist hingegen die Option „DEFENDO ruft zurück“ ausgewählt, so wird ein akzeptierter eingehender Ruf nicht angenommen sondern automatisch ein Rückruf an die Rufnummer ausgelöst, die unter „Anzuwählende Rufnummern“ angegeben wurde.

Hinweis:

Das B-Kanal Callback Verfahren, bei dem der DEFENDO den Ruf erst annimmt, den Benutzer authentifiziert und erst dann zurückruft ist nicht möglich.

Callback erfolgt immer an die Rufnummern die als „anzuwählende Rufnummern“ angegeben wurden egal von welcher (eingehenden) Rufnummer der Rückruf ausgelöst wurde.

Drücken Sie auf OK um Änderungen zu aktivieren oder drücken Sie auf Löschen um die gesamte Schnittstelle zu entfernen.

12.1.3. ISDN HDLC-RawIP

IP-Routen zu entfernten Netzwerken

Sind über die ISDN-Verbindung weitere Netzwerke angeschlossen, so können Sie hier die erforderlichen Routen zur Kommunikation mit diesen Netzwerken einrichten. Tragen Sie die Netzwerkadresse und die zugehörige Netzmaske des indirekt angeschlossenen Netzes ein. Als Gateway geben Sie bitte die IP-Adresse des ISDN-Routers der Gegenstelle ein. Drücken Sie auf Hinzufügen um die Route einzutragen. Sie geben auf diese Weise auch der Firewall bekannt, daß dieses Netzwerk über diese ISDN-Schnittstelle akzeptiert werden muß.

Konfigurierte Routen werden in folgendem Format angezeigt:

Netzwerkadresse/*Netzmaske*->*Gateway*

Um eine Route zu löschen, wählen Sie diese aus der Liste aus und drücken Sie auf Entfernen.

Anzuwählende Rufnummern

Geben Sie hier die Rufnummer ein, die angerufen werden soll. Beim Anschluß über eine Telefonanlage ist ggf. die Nummer der Amtsholung voranzustellen. Ist keine Rufnummer angegeben, so sind keine ausgehenden Rufe über diese Schnittstelle möglich.

Akzeptierte eingehende Rufnummern

Tragen Sie hier die Liste der Rufnummern ein, von denen eingehende Anrufe akzeptiert werden sollen. Bei Anrufern die das ISDN-Merkmal der Rufnummernübermittlung ausgeschaltet haben, wird als eingehende Rufnummer die 0 übermittelt.

Eingehende Anrufe von beliebigen Rufnummern akzeptieren

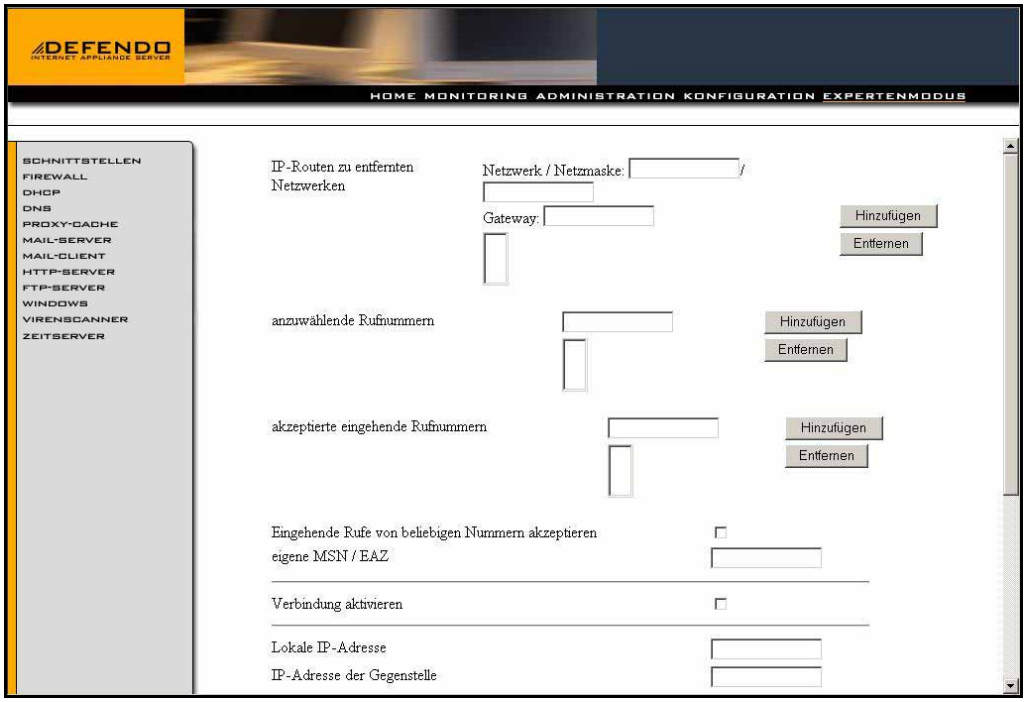
Wenn dieser Schalter aktiviert ist, werden alle eingehenden Anrufe von dieser Schnittstelle akzeptiert. Die Liste der akzeptierten eingehenden Rufnummern ist für diese Schnittstelle außer Kraft gesetzt. Sollten noch weitere Schnittstellen auf die gleiche MSN konfiguriert sein, ist nicht definiert, welche Schnittstelle den Anruf annimmt. Dies kann insbesondere zu Problemen bei der Fernwartung führen. Bitte verwenden Sie daher eine eigene MSN für Schnittstellen mit Rufnummern-Identifizierung sobald Sie auf einer Schnittstelle (egal ob ippp oder isdn) Anrufe von beliebigen Nummern akzeptieren.

Eigene MSN / EAZ

Geben Sie hier bitte die MSN bei Euro-ISDN bzw. die EAZ bei 1TR6 ein. Für das amerikanische NI1 Protokoll geben Sie bitte die MSN und den SPID im Format MSN:SPID an. Beim direkten Anschluß an einen NTBA der Telekom ist die MSN die komplette Rufnummer ohne Ortsvorwahl. Beim Anschluß an eine Telefonanlage ist die MSN häufig identisch mit der Durchwahl. Beim 1TR6-Protokoll darf hier nur genau eine Ziffer eingetragen werden, die im allgemeinen nichts mit der Durchwahl zu tun hat.

Verbindung aktivieren

Ist dieser Schalter deaktiviert, so werden eingehende und ausgehende Verbindungen über diese Schnittstelle unterbunden.



Lokale IP-Adresse

Geben Sie hier die IP-Adresse des DEFENDO ein, die er an dieser Schnittstelle haben soll. Bei der Fernwartungs-Schnittstelle isdn0 ist dieser Wert fest vorgegeben.

IP-Adresse der Gegenstelle

Geben Sie hier die IP-Adresse des ISDN-Routers der Gegenstelle ein. Bei der Fernwartungs-Schnittstelle isdn0 ist dieser Wert fest vorgegeben.

Kanalbündelung 128 kbit/s

Mit diesem Schalter aktivieren Sie die Kanalbündelung. Bei der Kanalbündelung wird der zweite ISDN-Kanal der ISDN-Karte bei entsprechend hoher Datentransferrate dynamisch zugeschaltet. Bitte beachten Sie, daß damit zwei ISDN-Leitungen belegt werden und damit auch die Telefongebühren für zwei Leitungen anfallen.

2. Kanal öffnen ab einer Transferrate von ... über eine Dauer von ...

Geben Sie hier die Transferrate in byte pro Sekunde und die Dauer in Sekunden ein für die diese Transferrate mindestens anliegen muß. Werden diese Werte überschritten, wird der 2. Kanal bei aktiver Kanalbündelung aufgeschaltet. Werden die Werte unterschritten, wird der 2. Kanal entsprechend der Einstellungen für den 1. Kanal wieder aufgelegt.

Standleitung an ISDN-Karte

Aktivieren Sie den Haken bei Standleitung und wählen Sie die zugehörige ISDN-Karte aus, wenn diese Schnittstelle an eine Standleitung angeschlossen ist.

Wählleitung

Aktivieren Sie den Haken bei Wählleitung wenn diese Schnittstelle nicht an eine Standleitung angeschlossen werden soll.

Dauer einer Einheit

Zur Optimierung der Verbindungstrennung tragen Sie hier bitte die Dauer einer Gebühreneinheit ein.

Zur nächsten Einheit auflegen wenn keine Datenübertragung in den letzten ... Sekunden

Werden in der hier eingegebenen Zeitspanne vor Ablauf der nächsten Zeiteinheit keine Daten mehr übertragen, wird die Verbindung automatisch getrennt.

Bei eingehenden Rufen muß die Gegenstelle auflegen

Diese Einstellung ist insbesondere bei RAS-Einwahlverbindungen sinnvoll. Bei eingehenden Rufen (also wenn der Anrufer die Gebühren zahlt) trennt DEFENDO die Verbindung nicht, auch wenn keine Daten mehr über diese Verbindung fließen.

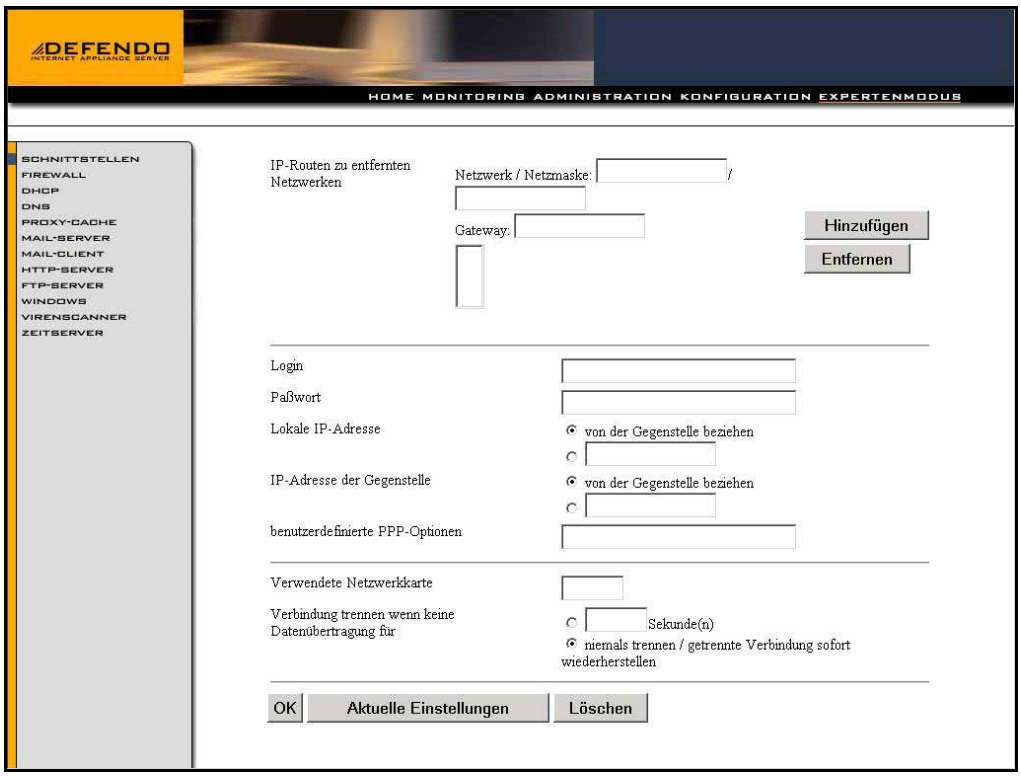
D-Kanal Callback

Sollten Sie die Wählleitung im D-Kanal Callback Verfahren betreiben wollen, so wählen Sie hier bitte die gewünschte Richtung aus. Bei der Auswahl von „Gegenstelle ruft zurück“ erwartet DEFENDO einen Rückruf, wenn der eigene Ruf von der Gegenstelle abgewiesen wurde. Ist hingegen die Option „DEFENDO ruft zurück“ ausgewählt, so wird ein akzeptierter eingehender Ruf nicht angenommen sondern automatisch ein Rückruf an die Rufnummer ausgelöst, die unter „Anzuwählende Rufnummern“ angegeben wurde.

> *Hinweis:*
>
> *Callback erfolgt immer an die Rufnummern die als „anzuwählende Rufnummern“ angegeben wurden egal von welcher (eingehenden) Rufnummer der Rückruf ausgelöst wurde.*

Drücken Sie auf OK um Änderungen zu aktivieren oder drücken Sie auf Löschen um die gesamte Schnittstelle zu entfernen.

12.1.4. ADSL / PPP over Ethernet



IP-Routen zu entfernten Netzwerken

Sind über die ADSL-Verbindung weitere Netzwerke angeschlossen, so können Sie hier die erforderlichen Routen zur Kommunikation mit diesen Netzwerken einrichten. Tragen Sie die Netzwerkadresse und die zugehörige Netzmaske des indirekt angeschlossenen Netzes ein. Als Gateway geben Sie bitte die IP-Adresse des Routers der Gegenstelle ein. Verwenden Sie die Adresse 0.0.0.0 bei dynamischer IP-Adresse. Drücken Sie auf Hinzufügen um die Route einzutragen. Sie geben auf diese Weise auch der Firewall bekannt, daß dieses Netzwerk über diese ISDN-Schnittstelle akzeptiert werden muß.

Konfigurierte Routen werden in folgendem Format angezeigt:

Netzwerkadresse/Netzmaske->Gateway

Um eine Route zu löschen, wählen Sie diese aus der Liste aus und drücken Sie auf Entfernen.

Login:

Geben Sie hier die Benutzerkennung ein, mit der sich der DEFENDO bei der Gegenstelle anmelden soll.

Paßwort

Geben Sie hier das Paßwort ein, mit dem sich der DEFENDO bei der Gegenstelle anmelden soll.

Lokale IP-Adresse

Wählen Sie von der Gegenstelle beziehen, wenn der DEFENDO die IP-Adresse von der Gegenstelle dynamisch zugewiesen bekommen soll. Wenn Sie die lokale IP-Adresse festlegen wollen, setzen Sie bitte den Haken vor dem Eingabefeld und tragen Sie die IP-Adresse des DEFENDO ein.

IP-Adresse der Gegenstelle

Wählen Sie von der Gegenstelle beziehen, wenn der DEFENDO die IP-Adresse der Gegenstelle dynamisch zugewiesen bekommen soll. Wenn der DEFENDO hingegen der Gegenstelle die IP-Adresse zuweisen soll oder die IP-Adresse der Gegenstelle fest definiert ist, setzen Sie bitte den Haken vor dem Eingabefeld und tragen Sie die IP-Adresse der Gegenstelle ein.

benutzerdefinierte PPP-Optionen

Je nach Gegenstelle sind in seltenen Fällen zusätzliche Optionen notwendig (z.B. das Deaktivieren bestimmter Kompressionsverfahren). Diese Optionen können hier angegeben werden. Dieses Feld ist in erster Linie für den Support gedacht.

Verwendete Netzwerkkarte

Tragen Sie hier die Netzwerkkarte ein, an die der Access-Concentrator für den PPP over Ethernet-Zugang angeschlossen wird (z.B. eth1). Diese Schnittstelle darf nicht als Ethernet-Schnittstelle konfiguriert sein. Sollte in der Schnittstellen-Hauptmaske die Schnittstelle bereits angelegt sein, so löschen Sie diese bitte vorher.

Verbindung trennen wenn keine Datenübertragung für ...

Eine DSL-Wählverbindung wird normalerweise automatisch aufgebaut, sobald Daten in das Internet übertragen werden sollen. Die Verbindung wird wieder getrennt, wenn während einer konfigurierbaren Zeitspanne keine Daten mehr über die Leitung übertragen wurden. Wählen Sie den entsprechenden Schalter um dieses Verhalten zu aktivieren. Wählen Sie den anderen Schalter, um eine getrennte Wählverbindung stets sofort wieder aufzubauen und diese bei Inaktivität nicht zu trennen.

Hinweis:

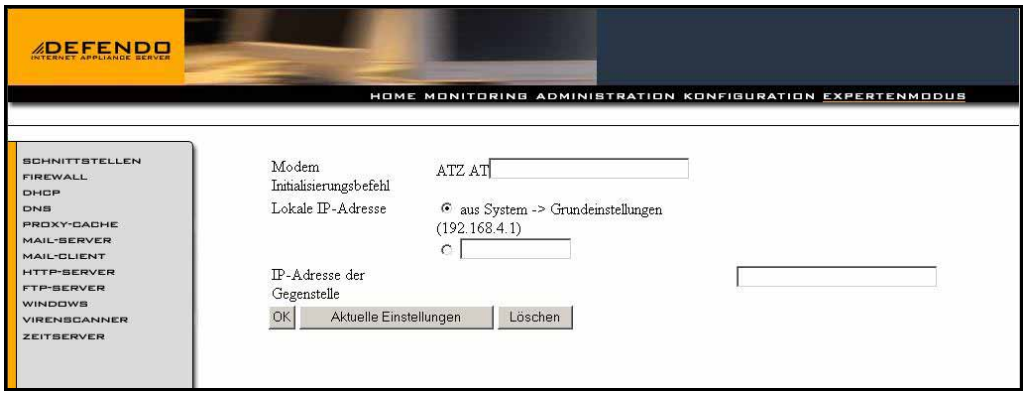
Aktivieren Sie die „niemals trennen“-Option nur, wenn die Internet-Verbindungen von Ihrem Service-Provider nicht zeitbasierend abgerechnet werden (Flatrate).

Häufig trennt der Service-Provider von sich aus die Leitung, wenn über einen bestimmten Zeitraum hinweg keine Daten übertragen werden. Möglicherweise wird die Verbindung auch getrennt, wenn die aktuelle Verbindungsdauer einen bestimmten Wert überschreitet.

Drücken Sie auf OK um Änderungen zu aktivieren oder drücken Sie auf Löschen um die gesamte Schnittstelle zu entfernen.

12.1.5. Serielles Modem

Derzeit ist dieser Schnittstellentyp nur für RAS-Einwahl gedacht.



Modem Initialisierungsbefehl

Zur Initialisierung wird dem Modem zunächst immer das ATZ-Kommando übermittelt. Ist ein weiterer Initialisierungsbefehl erforderlich, so geben Sie diesen bitte hier an (das führende AT ist dabei nicht mehr anzugeben).

Lokale IP-Adresse

Die lokale IP-Adresse kann aus den Grundeinstellungen übernommen werden. Wenn Sie eine andere Adresse eingeben wollen, so setzen Sie bitte den Haken vor dem Eingabefeld und tragen Sie dort die lokale IP-Adresse ein.

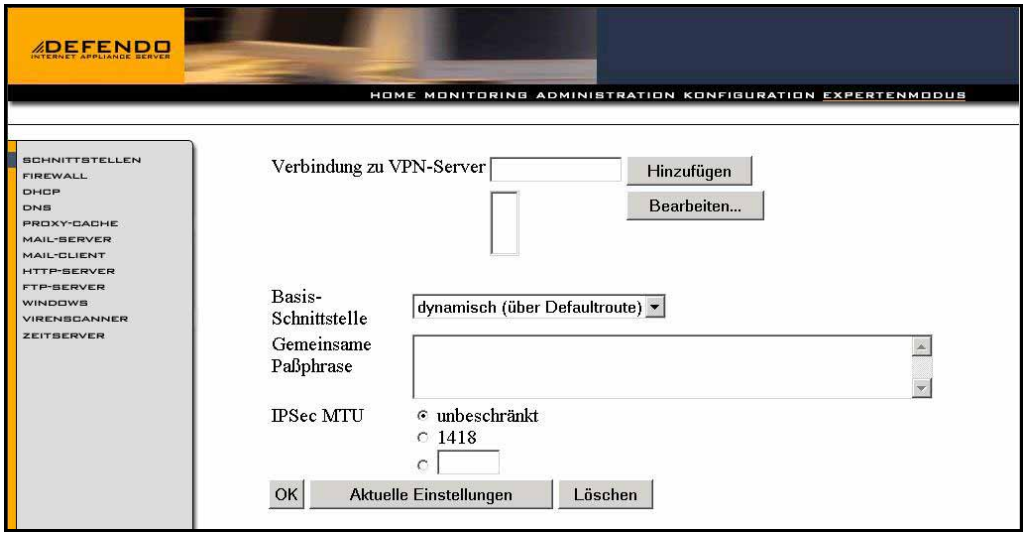
IP-Adresse der Gegenstelle

Tragen Sie hier die Adresse ein, die der DEFENDO der Gegenstelle zuweisen soll. Um den Einwähler mit Hilfe von Proxyarp-Routing transparent in eines der an den DEFENDO direkt angeschlossenen Netzwerke einzubinden, tragen Sie hier bitte eine freie Adresse aus dem gewünschten Netzwerk ein.

Drücken Sie auf OK um Änderungen zu aktivieren oder drücken Sie auf Löschen um die gesamte Schnittstelle zu entfernen.

12.1.6. VPN

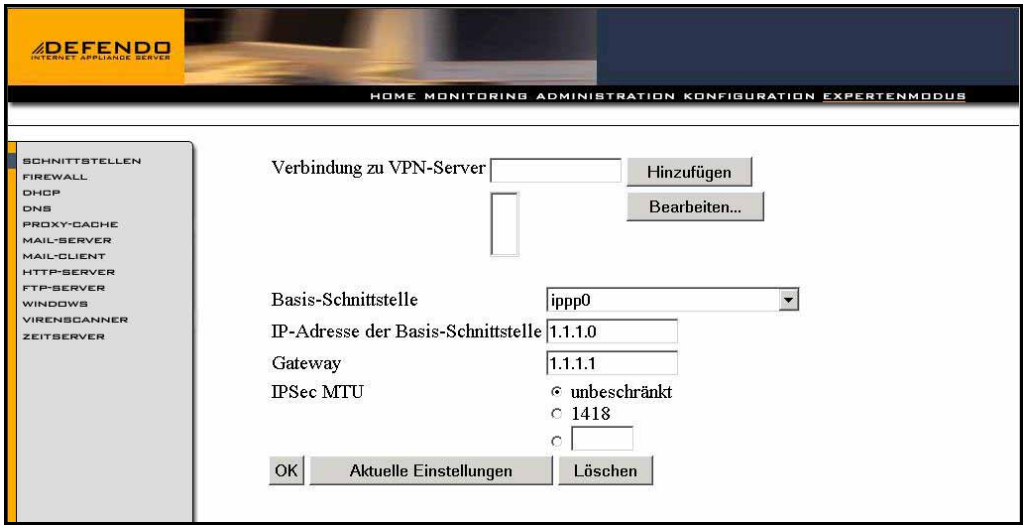
Im DEFENDO ist ein VPN-Server integriert, der sich weitgehend am IPSec-Standard orientiert. Der Aufbau eines VPNs erfolgt über das IKE-Protokoll (ISAKMP/Oakley) und kann über Shared-Secret oder RSA-Public-Keys authentifiziert werden. Die Verschlüsselung erfolgt stets mit Triple-DES (das vom IPSec-Standard vorgeschriebene Protokoll DES ist nicht verfügbar, da DES nicht mehr als sicher gilt). Als Hash-Algorithmen stehen MD5 oder SHA zur Verfügung. Die Paketauthentifizierung kann über das AH-Protokoll oder als Bestandteil der Verschlüsselung im ESP-Protokoll stattfinden. Um die Sicherheit der Verbindung zu erhöhen wird Perfect-Forward-Secrecy (PFS) eingesetzt. Hier werden die Diffie-Hellman Gruppen 2 und 5 (1024 und 1536 Bit Modulos) unterstützt. Die vom IPSec-Standard vorgeschriebene Unterstützung der Diffie-Hellman Gruppe 1 steht nicht zur Verfügung. Der Aufbau einer VPN-Verbindung im „Aggressive Mode“ wird nicht unterstützt. Auch virtuelle Identitäten sind nicht möglich.



Die VPN-Schnittstelle ist eine virtuelle Schnittstelle, die fest mit einer anderen Schnittstelle im System verknüpft wird (z.B. Ethernet-Schnittstelle). Über eine VPN-Schnittstelle lassen sich beliebig viele VPN-Verbindungen zu anderen VPN-Servern und VPN-Clients erstellen.

Nach dem Anlegen einer neuen ipsec-Schnittstelle werden Sie zunächst nach der gewünschten Basis-Schnittstelle gefragt. Verknüpfen Sie die VPN-Schnittstelle mit der Schnittstelle, über die der VPN-Server oder –Client der Gegenstelle erreicht werden kann. Im allgemeinen handelt es sich dabei um die Internet-Schnittstelle oder eine RAS-Schnittstelle des Systems. Sofern der DEFENDO über eine dynamische IP-Adresse an das Internet angebunden ist, muß die VPN-Schnittstelle ipsec0 angelegt und als Basis-Schnittstelle „dynamisch (über default-route)“ ausgewählt werden. Eine Nutzung weiterer ipsec-Schnittstellen wie z.B. ipsec1 ist dann nicht mehr möglich.

12.1.6.1. Die VPN-Hauptmaske



Verbindung zu VPN-Server

Wenn Sie eine Verbindung zu einem neuen VPN-Server oder -Client erstellen wollen, geben Sie hier bitte dessen IP-Adresse ein und drücken Sie auf den Schalter „Hinzufügen“. Hat dieser eine dynamische IP-Adresse, so verwenden Sie bitte die IP-Adresse „0.0.0.0“. Wollen Sie die Verbindungen zu einem bereits angelegten VPN-Server bearbeiten, so wählen Sie diesen bitte aus der Liste aus und drücken Sie auf „Bearbeiten“. In beiden Fällen wechseln Sie nun in die Maske zur Konfiguration der VPN-Verbindung mit dem gewählten Server.

Basis-Schnittstelle

Hier läßt sich die Schnittstelle ändern, mit der die ipsec-Schnittstelle verknüpft ist. Nur bei der Schnittstelle ipsec0 ist hier der Wert „dynamisch (über Defaultroute)“ auswählbar. Sofern der DEFENDO über eine dynamische IP-Adresse an das Internet angebunden ist, muß diese Einstellung gewählt werden. Es sind dann keine weiteren ipsec-Schnittstellen mehr verfügbar.

IP-Adresse der Basis-Schnittstelle

Tragen Sie hier bitte die IP-Adresse der ausgewählten Basis-Schnittstelle ein. Dieses Eingabefeld ist nicht vorhanden, wenn als Basis-Schnittstelle dynamisch eingestellt ist.

Gateway

Hier ist die IP-Adresse des Gerätes zu hinterlegen, das auf dem Weg vom DEFENDO zum gewählten VPN-Server als nächstes passiert wird. Im allgemeinen ist dies das Default-Gateway. Bei ISDN-Verbindungen ist hier die IP-Adresse der ISDN-Gegenstelle einzutragen. Dieses Eingabefeld ist nicht vorhanden, wenn als Basis-Schnittstelle dynamisch eingestellt ist.

Gemeinsame Paßphrase

Dieses Eingabefeld ist nur vorhanden, wenn als Basis-Schnittstelle dynamisch eingestellt ist. Wurde als Basis-Schnittstelle für das VPN „dynamisch (über Defaultroute)“ ausgewählt, so müssen alle VPN-Verbindungen die über eine gemeinsame Paßphrase (shared secret) authentifiziert werden, über die gleiche Paßphrase authentifiziert werden. Geben Sie diese hier ein. Eine gute Paßphrase ist möglichst lang und kompliziert aufgebaut (Sonderzeichen, Ziffern, Groß-/ Kleinschreibung). Sollte es nicht gewünscht sein, zu mehreren VPN-Servern die gleichen Authentifizierungsdaten zu verwenden, empfehlen wir RSA-Signaturen zur Authentifizierung zu verwenden.

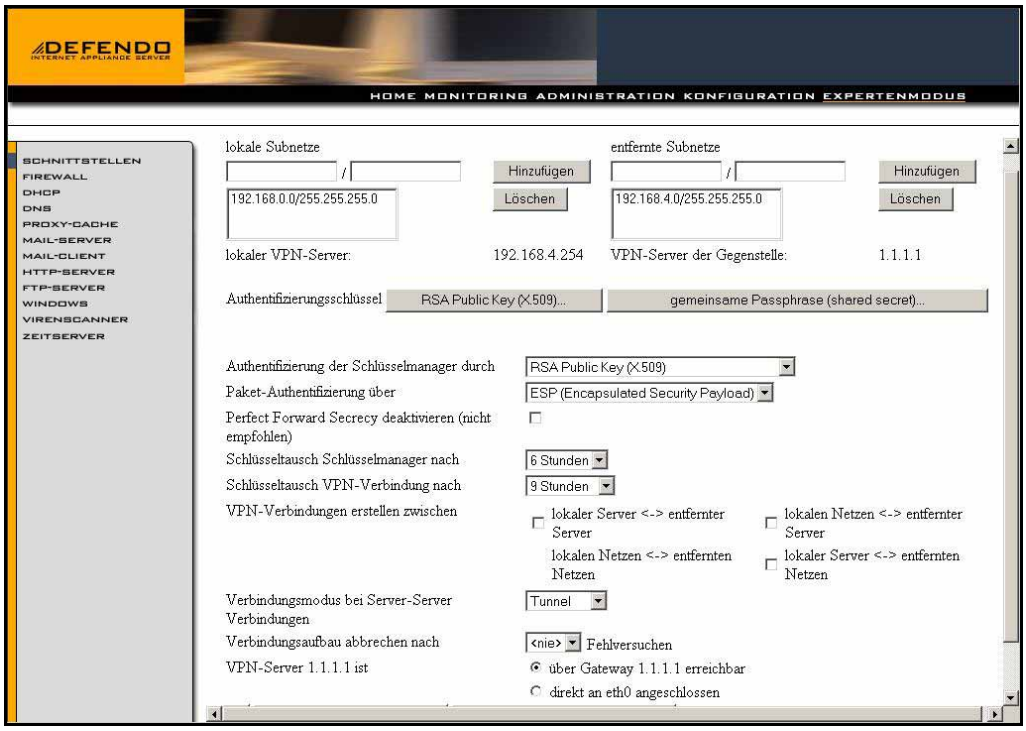
IPSec MTU

Wenn IP Pakete durch den IPSec-Header erweitert werden wird häufig die maximale Paketgröße überschritten die für den Verbindungsweg zum entfernten VPN-Server gilt. Die Pakete müssen daher Fragmentiert werden, was mit bestimmten Internet-Routern zu Problemen führen kann. Sollten VPN Verbindungsprobleme auftreten wenn Daten mit einem Volumen von mehr als 1500 Byte übermittelt werden, während Daten mit weniger als 1400 Byte problemlos übertragen werden sollten Sie versuchen den MTU Parameter zu beschränken. Beschränken Sie diesen Parameter zunächst auf 1418. Sie können jedoch auch einen beliebigen anderen Wert angeben wenn Sie die entsprechende Option

auswählen. Bei beschränkter MTU wird die Fragmentierung bereits durch die ipsec Schnittstelle des DEFENDO durchgeführt so dass während der Übermittlung zur Gegenstelle keine weitere Fragmentierung mehr notwendig sein sollte.

Wählen Sie OK um Änderungen in der Konfiguration zu aktivieren. Drücken Sie auf Löschen um die gesamte VPN-Schnittstelle mitsamt aller Verbindungen zu löschen.

12.1.6.2. Verbindung zu VPN-Servern mit fester IP



lokale Subnetze / entfernte Subnetze

Um IP-Netzwerke über VPN zu verbinden, geben Sie diese bitte als lokales bzw. entferntes Subnetz ein. IP-Pakete die von lokalen Subnetzen bzw. dem lokalen VPN-Server selbst kommen und an ein entferntes Subnetz bzw. an den VPN-Server der Gegenstelle gerichtet sind, können verschlüsselt über das VPN geleitet werden. Um ein neues Subnetz hinzuzufügen, spezifizieren Sie dieses zusammen mit der zugehörigen Netzmaske und drücken Sie auf „Hinzufügen“. Um einen einzelnen Rechner hinzuzufügen genügt es, dessen IP-Adresse anzugeben. Die Netzmaske ist dann nicht erforderlich. Die Adresse des lokalen VPN-Servers bzw. des VPN-Servers der Gegenstelle darf nicht unter den lokalen bzw. entfernten Subnetzen eingetragen werden.

Um eine VPN Verbindung ausschließlich zwischen den beiden beteiligten VPN-Servern zu erstellen, sind weder lokale noch entfernte Subnetze einzutragen. Entsprechend ist kein Eintrag bei den lokalen Subnetzen notwendig, wenn über VPN ausschließlich auf den lokalen VPN-Server zugegriffen wird. Wird ausschließlich auf den VPN-Server der Gegenstelle zugegriffen und nicht auf die Netzwerke dahinter ist kein entferntes Subnetz anzugeben.

Um die VPN-Verbindung zu einem Subnetz zu löschen, wählen Sie dieses bitte aus der entsprechenden Liste aus und drücken Sie auf „Löschen“.

Authentifizierungsschlüssel

Die Authentifizierung der Schlüsselmanager (IKE-Server) kann über public key-Verfahren mit X.509 Zertifikaten oder über eine gemeinsame Paßphrase erfolgen. Um das Zertifikat bzw. die Paßphrase festzulegen drücken Sie bitte den entsprechenden Schalter.

Sofern die VPN-Schnittstelle über eine dynamische IP-Adresse verfügt ist die gemeinsame Paßphrase bereits in der VPN-Hauptmaske anzugeben. Andernfalls erscheint nach Drücken des Schalters „gemeinsame Paßphrase (shared secret)...“ eine Eingabemaske, in der die Paßphrase eingegeben werden kann. Eine gute Paßphrase ist möglichst lang und kompliziert aufgebaut (Sonderzeichen, Ziffern, Groß-/ Kleinschreibung). Drücken Sie „OK“ um die Paßphrase zu speichern, „Löschen“ um die Paßphrase zu entfernen.

Der Beschreibung der Authentifizierung „RSA public key (X.509)“ ist ein eigenes Kapitel gewidmet. Lesen Sie dazu bitte das Kapitel 12.1.6.4.

Authentifizierung der Schlüsselmanager über

Wählen Sie hier bitte aus, wie sich die Schlüsselmanager gegenseitig authentifizieren sollen. Zur Verfügung stehen die Authentifizierung mit RSA-Keys und die Authentifizierung über eine gemeinsame Paßphrase (shared secret). Die Authentifizierung über RSA public keys ist zwar umfangreicher zu konfigurieren, ist jedoch konzeptionell sicherer.

Bei der Verwendung des public key Verfahrens mit X.509 Zertifikaten verfügt jeder beteiligte VPN-Server über einen privaten und einen öffentlichen Schlüssel. Der private Schlüssel muß unbedingt geheim bleiben. Der öffentliche Schlüssel ist an jeden VPN-Server zu übermitteln, mit dem eine VPN-Verbindung erstellt werden soll.

Wird die gemeinsame Paßphrase zur Authentifizierung verwendet, so ist für jeden VPN-Server mit dem kommuniziert wird eine solche Paßphrase einzutragen. Diese ist unbedingt geheim zu halten. Da die Paßph-

rase sowohl dem lokalen VPN-Server als auch dem VPN-Server der Gegenstelle bekannt sein muß, ist diese auf einem sicheren Weg dem anderen VPN-Server zu übermitteln.

Paketauthentifizierung über

Die Authentifizierung kann als Bestandteil der Verschlüsselung stattfinden. Wählen Sie dazu „Encapsulated Security Payload (ESP)“. Alternativ kann die Paketauthentifizierung mit einem eigenständigen Protokoll erfolgen. Wählen Sie dazu „Authentication header (AH)“.

Perfect Forward Secrecy deaktivieren

Durch aktivieren der zugehörigen Schaltfläche wird Perfect Forward Secrecy deaktiviert. Gelangt ein Angreifer nachträglich an die gemeinsame Passphrase bzw. an die privaten Schlüssel eines mit RSA-Zertifikaten gesicherten VPN’s, so kann er eine aufgezeichnete VPN-Verbindung entziffern. Es empfiehlt sich daher nicht, Perfect Forward Secrecy zu deaktivieren. Für die Interoperabilität mit anderen VPN-Server-Implementierungen kann dies jedoch notwendig werden.

Achtung:

Perfect Forward Secrecy sollte nur deaktiviert werden, wenn dies unbedingt notwendig ist!

Schlüsseltausch Schlüsselmanager

Wählen Sie hier die Zeitspanne aus, nach der der Schlüssel des an dieser VPN-Verbindung beteiligten Internet-Key-Exchange-Server neu vereinbart wird.

Schlüsseltausch VPN-Verbindung

Wählen Sie hier die Zeitspanne aus, nach der der Schlüssel für die VPN-Verbindung neu vereinbart wird.

VPN Verbindungen erstellen zwischen

Zwischen zwei VPN-Servern können bis zu vier Verbindungen konfiguriert werden. Eine Verbindung ist stets aktiv. Je nachdem ob bei den lokalen Subnetzen und oder den entfernten Subnetzen weiter oben in dieser Maske Einträge aufgenommen wurden, lassen sich die anderen Verbindungen zusätzlich aktivieren. Aktivieren Sie dazu die entsprechenden Auswahlfelder. Folgende Verbindungen stehen zur Verfügung:

Lokaler Server – entfernter Server: Die Kommunikation zwischen den beiden Servern selbst erfolgt über VPN. Die VPN-Verbindung verwendet dabei jeweils die externe IP-Adresse des VPN-Servers (die IP-Adresse der Basisschnittstelle).

Lokale Netze – entfernter Server: Die VPN-Verbindung wird zwischen den IP-Adressen aus den lokalen Netzen und der (externen) IP-Adresse des VPN-Servers der Gegenstelle erstellt.

Lokale Netze – entfernte Netze: Die lokalen und entfernten Netze werden über VPN verbunden.

Lokaler Server – entfernte Netze: Die VPN-Verbindung besteht zwischen den IP-Adressen aus den entfernten Netzen und der (externen) IP-Adresse des DEFENDO.DEFENDODEFENDO

Verbindungsmodus bei Server-Server Verbindungen

Wählen Sie Tunnel wenn die VPN-Verbindung zwischen den beiden VPN-Servern mit Hilfe von ESP-Paketen getunnelt werden soll. Dabei werden die Original-Pakete verschlüsselt in neue Pakete eingebettet. Wählen Sie Transport wenn die Verbindung direkt über AH-Pakete abgewickelt werden soll.

Verbindungsaufbau abbrechen nach

Wählen Sie hier die Anzahl der Versuche aus, die maximal unternommen werden eine VPN-Verbindung mit der Gegenstelle aufzubauen. Bitte beachten Sie, daß die Auswahl von <nie> bei Wählverbindungen unter Umständen mit hohen Gebühren verbunden ist.

VPN-Server ... ist über Gateway erreichbar

Wählen Sie „ist direkt an ... angeschlossen“, wenn der angesprochene VPN-Server physikalisch am gleichen Netzwerk angeschlossen ist wie der DEFENDO. Andernfalls ist die Einstellung „ist über Gateway ... erreichbar“ auszuwählen. Ist die IP-Adresse des DEFENDO dynamisch, ist diese Einstellung nicht verfügbar.

Drücken Sie auf OK um Änderungen in der Konfiguration zu aktivieren. Um alle Verbindungen mit dem aktuellen VPN-Server zu entfernen, drücken Sie bitte auf „VPN-Verbindung löschen“.

12.1.6.3. Verbindung zu VPN-Servern mit dynamischer IP

Der DEFENDO kann zu mehreren VPN-Server mit dynamischer IP-Adresse eine VPN-Verbindung erstellen. Es kann sich dabei sowohl um einen einzelnen Client mit VPN-Software handeln (z.B. Notebook des Außendienstmitarbeiters) als auch um einen VPN-Server der die Kommunikation zu einem entfernten Subnetz ermöglicht. Um diese recht un-

terschiedlichen Szenarien kennzeichnen zu können und um VPN-Verbindungen mit identischer Konfiguration zusammenzufassen (Außendienstmitarbeiter!), lassen sich die Konfigurationen unter einem frei zu vergebenden Verbindungsnamen erstellen. Der Verbindungsname darf aus Buchstaben, Ziffern und Punkten bestehen. Umlaute sind nicht erlaubt. Geben Sie einen Verbindungsnamen ein und drücken Sie auf „Hinzufügen“ um eine neue Konfiguration für VPN-Verbindungen zu Servern mit dynamischer IP-Adresse anzulegen. Wählen Sie einen Verbindungsnamen aus der Liste aus und drücken Sie auf „Bearbeiten“ um die zugehörige Konfiguration anzupassen.

Die Einstellungen in der hierauf folgenden Maske entsprechen weitgehend den Einstellungen für Verbindungen zu VPN-Servern mit statischer IP-Adresse (vgl. Kapitel 12.1.6.2). Abweichend von der dortigen Beschreibung lassen sich jedoch beliebig viele X.509-Zertifikate hinterlegen. Auf diese Weise ist es z.B. möglich, den Zugriff von mehreren Außendienstmitarbeitern durch einfaches Hinzufügen oder Entfernen von Zertifikaten zu konfigurieren. Um ein neues X.509-Zertifikat hinzuzufügen, geben Sie im Bereich „Authentifizierungsschlüssel“ einen beliebigen Namen für dieses Zertifikat an und drücken Sie auf „Hinzufügen“. Der Name darf aus Buchstaben, Ziffern und Punkten bestehen. Umlaute sind nicht zulässig. Um ein bestehendes Zertifikat zu ändern oder zu löschen, wählen Sie es aus der Liste aus und drücken Sie auf „Bearbeiten“.

Gemeinsame Paßphrase (shared secret)

Sofern die VPN-Server mit dynamischer IP-Adresse über shared secret authentifiziert werden sollen, ist hier die zu verwendende Paßphrase anzugeben. Bitte beachten Sie, daß alle VPN-Server mit dynamischer IP-Adresse die selbe Paßphrase verwenden müssen. Eine eindeutige Authentifizierung der Gegenstelle ist nicht möglich. Eine spätere Änderung der Paßphrase erfordert damit z.B. die Änderung auf allen VPN-Servern mit denen kommuniziert wird. Es empfiehlt sich daher die Authentifizierung über RSA-Zertifikate.

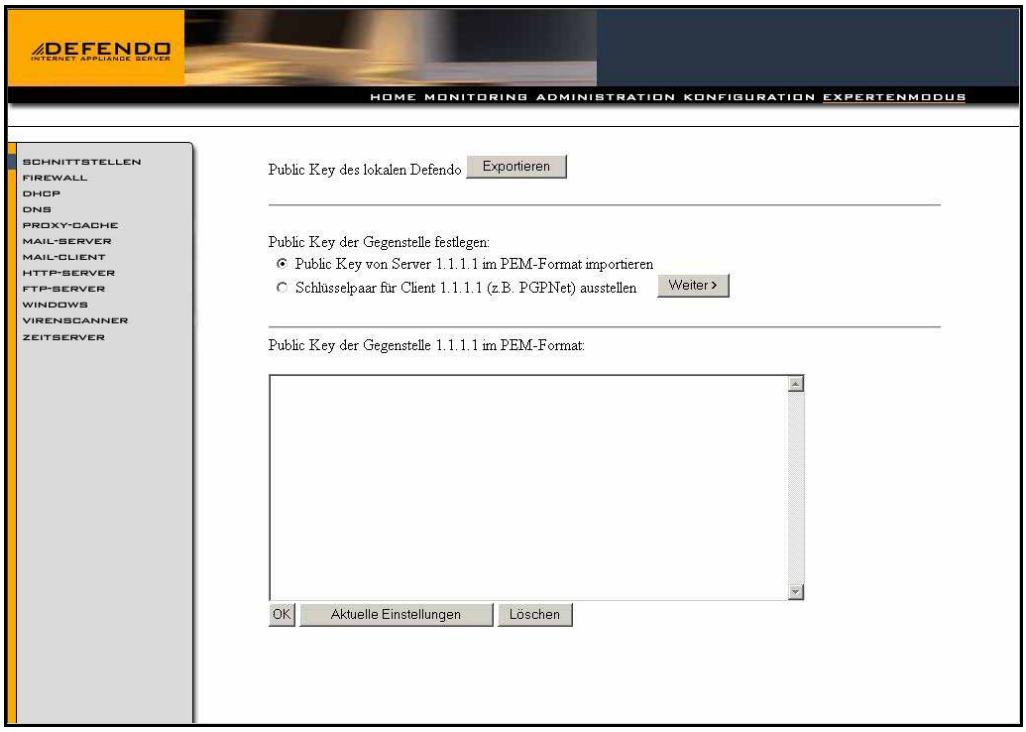
Drücken Sie auf „OK“ um die Änderungen zu übernehmen oder „Alle löschen“ um die VPN-Verbindungen zu allen Servern mit dynamischer IP-Adresse zu trennen.

Achtung:

Ein Szenario in dem sowohl der lokale DEFENDO als auch die Gegenstelle über dynamische IP-Adressen verfügen ist nicht möglich.

Verfügt die Gegenstelle über eine dynamische IP-Adresse, so muß stets die Gegenstelle die VPN-Verbindung initiieren. Erst dann kann vom lokalen DEFENDO auf die Gegenstelle zugegriffen werden und auch nur so lange bis die Gegenstelle die Internet-Verbindung trennt. Anschließend muß die Gegenstelle erneut die VPN-Verbindung initiieren.

12.1.6.4. X.509-Zertifikat festlegen



Die Authentifizierung der VPN-Schlüsselmanager kann über RSA public keys erfolgen. Wird dieses Authentifizierungsverfahren gewählt, muß jeder VPN-Server über ein eigenes Schlüsselpaar bestehend aus dem privaten und dem öffentlichen Schlüssel verfügen (private und public key). Der private Schlüssel ist dabei nur dem Server bekannt zu dem er gehört und ist unbedingt geheim zu halten. Damit zwei Server sich gegenseitig authentifizieren können, müssen diese Ihre öffentlichen Schlüssel untereinander austauschen. Die öffentlichen Schlüssel brauchen dabei nicht geheim gehalten zu werden. Damit die Authentifizie-

rung über die Zertifikate vorgenommen kann ist also folgender Zustand herzustellen:

- VPN-Server A verfügt über einen privaten Schlüssel der nur A bekannt ist und A eindeutig identifiziert
- VPN-Server B verfügt über einen privaten Schlüssel der nur B bekannt ist und B eindeutig identifiziert
- VPN-Server A verfügt über den öffentlichen Schlüssel von B (der zum privaten Schlüssel von B gehört).
- VPN-Server B verfügt über den öffentlichen Schlüssel von A (der zum privaten Schlüssel von A gehört).

Privater Schlüssel des DEFENDO

Jeder DEFENDO verfügt bereits über ein X.509 RSA-Schlüsselpaar mit einem eindeutigen privaten Schlüssel. Der Import und Export sowie die Erstellung eines neuen Schlüsselpaares ist möglich (vgl. Kapitel 9.5).

Achtung:

Aus Sicherheitsgründen ist das Schlüsselpaar des DEFENDO nicht im System-Backup enthalten. Nutzen Sie bitte die Export-Funktion aus Kapitel 9.5.4 um diesen geschützt zu speichern.

Public Key des lokalen DEFENDO

Dem VPN-Server der Gegenstelle muß der öffentliche Schlüssel des DEFENDO bekannt gemacht werden. Der Schalter „Exportieren“ DEFENDO ermöglicht es Ihnen, diesen Schlüssel im PEM-Format abzuspeichern. Er kann dann z.B. per Mail oder Diskette an die Gegenstelle übermittelt werden. Dieser Transfer muß nicht speziell abgesichert werden. In diesem Bereich wird auch das Subject und die Gültigkeitsdauer des DEFENDO Zertifikates angezeigt.

Public Key der Gegenstelle festlegen

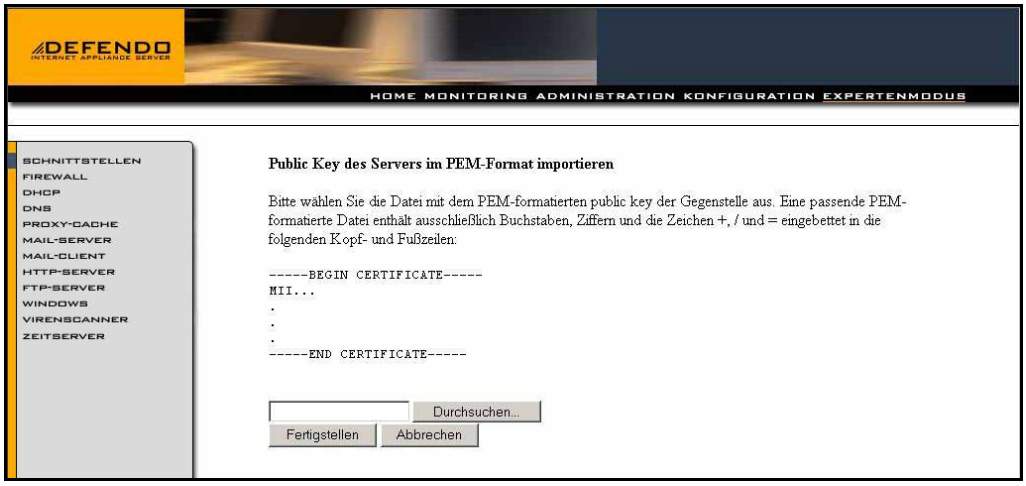
Liegt der öffentliche Schlüssel der Gegenstelle im PEM-Format auf Ihrem lokalen Computer, läßt sich dieser direkt importieren. Wählen Sie dazu den Optionsschalter „Public key von Server ... im PEM-Format importieren“ und drücken Sie auf „Weiter“. Wählen Sie dann mit Hilfe der „Durchsuchen“ Schaltfläche die Datei mit dem PEM-formatierten öffentlichen Schlüssel aus und drücken Sie auf „Fertigstellen“ um die Datei an den DEFENDO zu übermitteln. Nutzen Sie dieses Verfahren, wenn es sich bei der Gegenstelle z.B. ebenfalls um einen DEFENDO handelt.

Läßt sich bei der Gegenstelle der öffentliche Schlüssel nicht im PEM-Format exportieren, so kann der DEFENDO ein komplettes Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel für die Gegenstelle generieren. Wählen Sie dieses Verfahren, wenn Sie z.B. einen PGPNet VPN-Client mit dem DEFENDO verbinden wollen. Aktivieren Sie dazu den Optionsschalter „Schlüsselpaar für Client ... ausstellen“ und drücken Sie auf den Schalter „Weiter“. In der folgenden Maske können Sie die Daten für das zu erstellende X.509-Zertifikat eingeben. Hier muß ferner ein Import-Paßwort eingegeben werden Der generierte private Schlüssel wird durch das Import-Paßwort geschützt und kann später nur mit diesem Import-Paßwort in die VPN-Software der Gegenstelle importiert werden. Drücken Sie auf die „Weiter“-Schaltfläche um das neue Schlüsselpaar zu generieren. Auf der folgenden Seite kann das Schlüsselpaar mit dem paßwortgeschützten privaten Schlüssel exportiert werden. Drücken Sie die entsprechende Schaltfläche um das Schlüsselpaar im PKCS12-Format abzuspeichern. Übermitteln Sie diese Datei später an die Gegenstelle und importieren Sie sie in die VPN-Software der Gegenstelle. Wenn Sie schließlich auf die Schaltfläche „Fertigstellen“ drücken, wird der öffentliche Schlüssel des generierten Schlüsselpaares automatisch vom DEFENDO als öffentlicher Schlüssel der Gegenstelle gespeichert. Der generierte private Schlüssel der Gegenstelle wird auf dem DEFENDO gelöscht.

Public Key der Gegenstelle ... im PEM-Format

In diesem Bereich werden zum öffentlichen Schlüssel der Gegenstelle das Subject, die Gültigkeitsdauer sowie der öffentliche Schlüssel selbst im PEM-Format angezeigt. Über die Cut-and-Paste-Funktion läßt sich ein public key im PEM-Format im Textfeld eintragen. Der Schlüssel muß stets folgendes Format haben:

-----BEGIN CERTIFICATE-----
MII...
.
.
.
-----END CERTIFICATE-----



Wählen Sie „OK“ um den öffentlichen Schlüssel zu übernehmen oder „Löschen“ um den öffentlichen Schlüssel zu entfernen.

12.2. Firewall

Die Administration der Firewall sollte ausschließlich von Fachleuten durchgeführt werden. Unbedachte Änderungen können die Sicherheit des DEFENDO sowie aller daran direkt oder indirekt angeschlossenen Netzwerkgeräte beeinträchtigen.

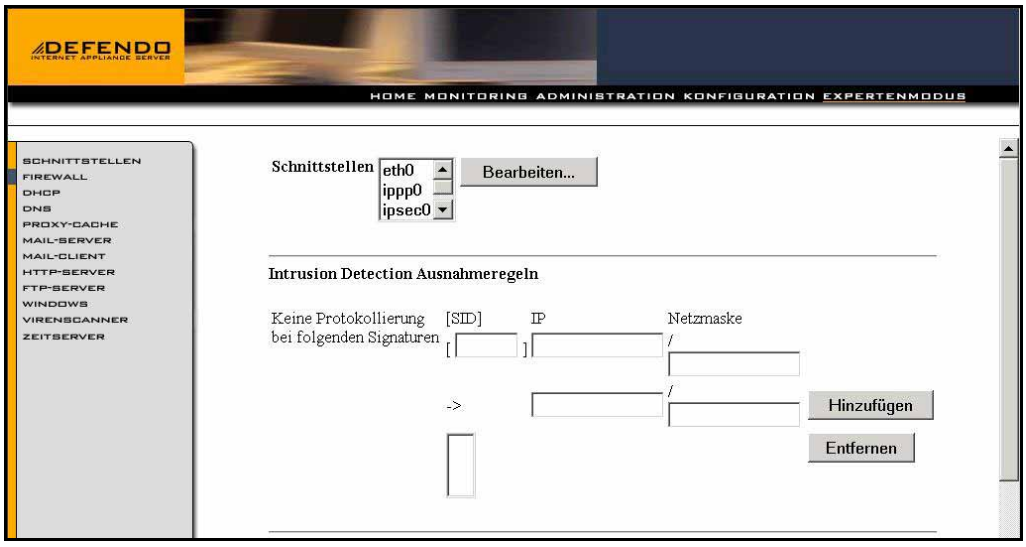
Über das Firewall-Menü werden folgende Komponenten konfiguriert:

- Die standard Firewall: Diese ist bei allen Modellen integriert. Es handelt sich um einen Paket-Filter mit stateful inspection und Network-Adress-Translation (NAT / SNAT). Aufgrund der eingetragenen Routen und der IP-Adressen der Schnittstelle erkennt die Firewall, welche Netzwerke über welche Schnittstelle erreichbar sind und aktzeptiert auch nur diese Adressen als gültig. Sogenanntes Adress-Spoofing wird damit unterbunden. Aus Sicherheitsgründen werden ferner alle Pakete defragmentiert. Pakete mit Source-Routing-Informationen werden verworfen.
- Das Portforwarding (DNAT): Dieses ermöglicht den transparenten Zugriff aus dem Internet auf dem Server in einem vor dem Internet verborgenen IP-Adressbereich.
- Die dynamische Firewall: Diese basiert auf Sensoren, die eigenständig Zugriffe bewerten und diese Bewertungen an die zentrale Steuerkomponent melden. Diese leitet konfigurierbare Gegenmaßnahmen ein. Die Komponenten der dynamischen Firewall unterscheiden dabei 4 verschiedene Zeithorizonte. Im Bereich von Millisekunden agieren die Sensoren autark, um

unmittelbar auf Angriffe eingehen zu können. Dieses Verhalten ist nicht weiter konfigurierbar. Die umfangreichsten Konfigurationsmöglichkeiten stehen hingegen für den „kurzfristigen“ Zeitbereich von Sekunden bis Minuten zur Verfügung. Angriffe die sich über einen Zeitraum von Minuten bis zu ca. 24h erstrecken, werden als „mittelfristig“ bezeichnet. Hierbei besteht die Möglichkeit, dass deren Ursprung eine dynamische IP-Adresse ist und somit langfristige Gegenmaßnahmen fehl am Platze sind. Der langfristige Bereich hingegen betrifft Adressen, die über mehrere Tage hinweg auffällig werden. Hier ist von festen IP-Adressen auszugehen.

- Intrusion Detection: Diese Komponente erkennt auf Basis einer Datenbank potentiell gefährliche Datenpakete. Die Klassifikation erfolgt anhand von TCP/IP-Header-Daten wie z.B. der beteiligten Ports als auch anhand des eigentlichen Inhalts der Datenpakete. Die Intrusion Detection ist eine passive Komponente, die folglich verdächtige Verbindungen lediglich aufzeichnet, nicht jedoch unterbricht.

12.2.1. Die Firewall-Hauptmaske



Schnittstellen

Im Bereich Schnittstellen wird die Konfiguration der Standard-Firewall vorgenommen. Die Administration der Standard-Firewall erfolgt Schnittstellen basierend. Um den IP-Paketfluß von Paketen zu reglementieren, die an den DEFENDO selbst gerichtet sind, wählen Sie bitte die Schnittstelle, über die die Pakete eingehen. Entsprechen konfigurieren Sie für Pakete die Ihren Ursprung im DEFENDO selbst haben die

Schnittstelle, über die das Paket den DEFENDO verläßt. Für Pakete die durch den DEFENDO hindurchgeleitet werden konfigurieren Sie bitte ebenfalls die Schnittstelle, über die das Paket den DEFENDO wieder verläßt.

Wählen Sie unter Schnittstellen die Schnittstelle aus, die Sie konfigurieren wollen und klicken dann auf „Bearbeiten“.

Intrusion Detection Ausnahmeregeln

Die Komponente Intrusion Detection protokolliert alle verdächtigen Datenpakete die gemäß der aktivierten Signaturdatenbanken erkannt werden. Im Protokoll der Intrusion Detection (vgl. Kapitel 11.2.4.4) wird zu jeder erkannten Attacke u.a. die Quell-IP, die Ziel-IP und die Signaturnummer (SID) angezeigt.

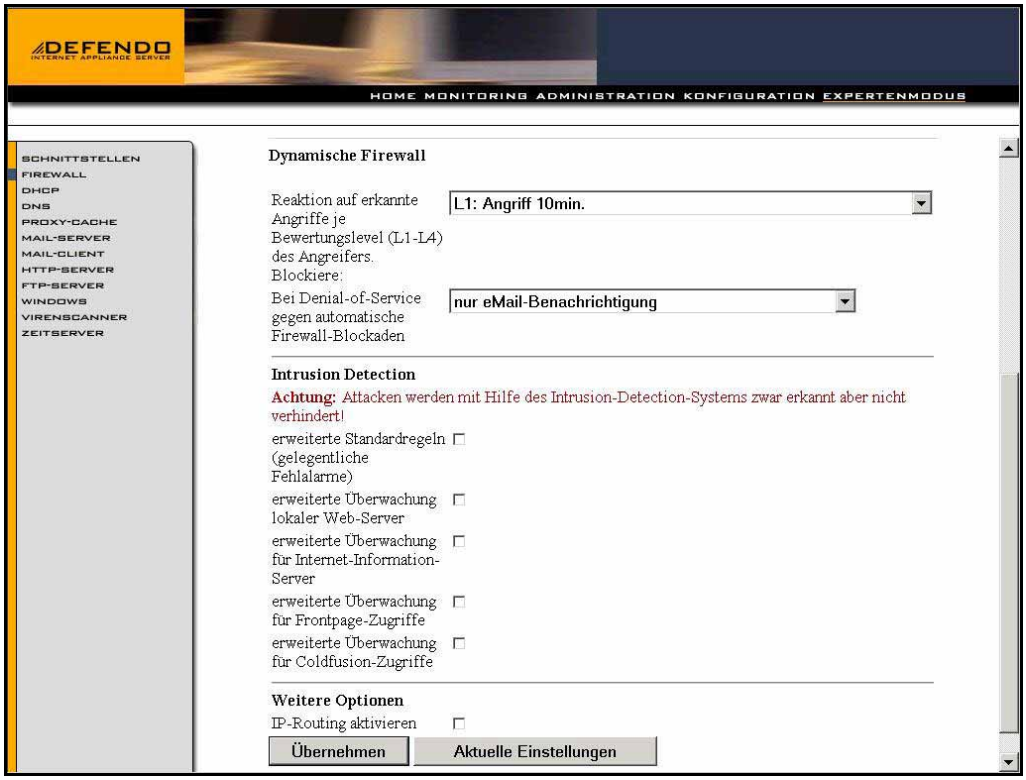
Achtung:

Bitte beachten Sie, dass hier nur SIDs zur Modul-Nummer 1 angegeben werden können. Beispielsweise bedeutet [1:499:2] Modul-Nummer 1, SID 499, Revision 2. Da es sich um eine SID zu Modul-Nummer 1 handelt kann in diesem Falle die 499 als SID eingetragen werden. Erhalten Sie im Protokoll hingegen z.B. [2:7:1] so kann hier keine passende Regel eingegeben werden, da die Meldung nicht durch das Signatur-Datenbank-Modul sondern durch das Modul mit ID 2 erzeugt wurde.

In dieser Maske kann die Protokollierung basierend auf der Signaturnummer (SID) und Quell- bzw. Ziel-IP-Adressen deaktiviert werden. Geben Sie dazu die SID sowie die Quell- und Ziel-Adressen des Paketes in die entsprechenden Felder ein. Bei der Angabe einer einzelnen IP-Adresse als Quelle bzw. Ziel kann das zugehörige Netzmasken-Feld leer bleiben. Um ganze IP-Subnetze anzugeben tragen Sie bitte die Netzwerkadresse sowie die zugehörige Netzmaske ein. Lassen Sie die Quelle bzw. das Ziel frei wenn die Regel für beliebige IP-Adressen gelten soll. Entsprechend können Sie auch eine Regel ohne SID spezifizieren. Die Regel gilt dann für alle Signaturen. Auf diese Weise können Sie z.B. einzelne IP-Adressen komplett von der Protokollierung auszunehmen. Drücken Sie auf „Hinzufügen“ um einen neue Regel zu aktivieren. Wählen Sie eine Regel aus der Liste und drücken Sie auf „Entfernen“ um darauf passende Pakete wieder zu Protokollieren.

Hinweis:

Wird die SID einer recht unspezifischen Signatur angegeben, so kann es sein, dass damit auch andere, spezifischere Signaturen ausgeblendet werden.



Dynamische Firewall

In diesem Bereich werden die schnittstellen-übergreifenden Einstellungen der dynamischen Firewall vorgenommen.

Im Bereich „Reaktion auf erkannte Angriffe je Bewertungslevel“ werden die Gegenmaßnahme auf Angriffe im kurzfristigen Zeitbereich (Sekunden bis Minuten) eingestellt. Hier besteht jeweils die Möglichkeit, die Ursprungs-IP-Adresse des Angreifers komplett für einen definierten Zeitraum zu blockieren. Die abgeschwächtere Variante ist die Blockade des Angriffs. Hier wir nicht die komplette Quell-Adresse gesperrt sondern lediglich die Pakete die auf den erkannten Angriff passen (z.B. bei einer erkannten Denial-of-Service Attacke an den gleichen Zielport gerichtet sind). Die Bewertungslevel (L1-L4) sind mit einem Schwellwert verknüpft. Die zu diesem Level gehörende Maßnahme wird eingeleitet, wenn die von den Sensoren vorgenommene Bewertung der Zugriffe einer IP-Adresse den Schwellwert überschreitet.

Ein Angreifer könnte das Verhalten der dynamischen Firewall – nämlich das Sperren von IP-Adressen – ad absurdum führen, indem er durch

eine Vielzahl von Paketen mit gefälschten Absenderadressen in rascher Folge ganze Bereiche des Internets aussperrt. Wird ein solcher Angriff erkannt, wird die unter „Bei Denial-of-Service gegen automatische Firewall-Blockaden“ ausgewählte Aktion durchgeführt.

Intrusion Detection

Der Schalter „Erweiterte Standardregeln (gelegentliche Fehlalarme)„ erweitert die Regelbasis der Intrusion Detection. Standardmäßig werden lediglich Pakete erkannt, die aufgrund Ihrer Signatur ziemlich eindeutig auf gefährlichen Datentransfer hinweisen. Mit den erweiterten Standardregeln aktivieren Sie weitere Regeln, die auch Pakete erkennen die eine verdächtige Signatur aufweisen, jedoch durchaus auch im normalen Betrieb auftreten könnten. Fehlalarme sind in diesem Falle also durchaus möglich.

Auch der Schalter „Erweiterte Überwachung lokaler Webserver“ erweitert die Regelbasis. Zugriffe auf Webserver werden auf diese Weise auf bestimmte Angriffs- oder Mißbrauchssignaturen überwacht. Diese Regeln sind nur dann wichtig, wenn auch tatsächlich ein Internet-Webserver in einem der an den DEFENDO angeschlossenen Netzwerke aktiv ist.

Sollten Sie Microsoft Internet-Information-Server als Internet-Webserver betreiben und an einem vom DEFENDO überwachten Netzwerk angeschlossen haben, so aktivieren Sie mit dem Schalter „Erweiterte Überwachung für Internet-Information-Server“ spezielle Signaturen für Angriffe auf diese Syteme.

Bei Aktivierung des Schalters „Erweiterte Überwachung für Frontpage-Zugriffe“ werden bestimmte Zugriffe mit Microsoft Frontpage protokolliert, bei Aktivierung von „Erweiterte Überwachung für Coldfusion-Zugriffe“ Zugriffe der Coldfusion Software.

IP-Routing aktivieren

Mit Hilfe dieses Schalters können Sie das IP-Routing aktivieren. Ist das IP-Routing deaktiviert, so sind unabhängig von den konfigurierten Firewall-Regeln ausschließlich Verbindungen zu oder vom DEFENDO möglich. Verbindungen durch den DEFENDO hindurch sind vollständig unterbunden. Es erfolgt in diesem Fall auch keine Protokollierung dieser Pakete durch den Firewall.

12.2.2. Die Firewall-Schnittstellen Maske

Zur Erleichterung der Firewall-Konfiguration bietet Ihnen der DEFENDO vier Templates für Vertrauensstufen an. Je nachdem an welches Netz eine Schnittstelle angeschlossen ist, können Sie das Vertrauen in Pakete die über diese Schnittstelle fließen in eine der folgenden Kategorien einordnen:

- **kein Vertrauen:**

  Diese Stufe wird typischerweise dann vergeben, wenn die Schnittstelle direkt mit dem Internet verbunden ist. Direkte Verbindungen aus Netzen mit hohem oder mittlerem Vertrauen werden dabei mit Hilfe der Network Adress Translation (NAT) manipuliert. Die IP-Adresse des eigentlichen Absenders wird dabei im DEFENDO durch die Adresse der Schnittstelle ersetzt, über die das Paket den DEFENDO verläßt. Wenn erforderlich wird dabei der UDP- bzw. TCP-Port des Absenders verändert, um die Eindeutigkeit einer Verbindung zu gewährleisten. Bei Antwortpaketen werden entsprechend wieder die Originalwerte eingetragen. Auf diese Weise ist es zum einen möglich, daß sich mehrere Geräte aus dem lokalen Netz über nur eine IP-Adresse mit dem Internet verbinden. Zum anderen bleiben die internen IP-Adressen gegenüber dem Internet verborgen.

- **geringes Vertrauen:**

  Für diese Stufe gibt es zwei mögliche Anwendungsfälle. Der typische Fall ist die Einrichtung einer sogenannte demilitarisierten Zone (DMZ). In einer DMZ werden Server aufgestellt, auf die gezielter Zugriff aus dem Internet möglich sein soll (z.B. Mail- oder Webserver). Das zweite aber eher seltene Anwendungsbeispiel ist der Anschluß der Schnittstelle an das Internet über

eine vorgelagerte Firewall mit hohem Sicherheitsstandard. Network Adress Translation kommt bei dieser Einstellung nicht zum Einsatz.

- **mittleres Vertrauen:**
  Typische Anwendungsfälle sind Remote Access Schnittstellen oder LAN-Bereiche bei denen der Zugriff in andere Netzwerkbereiche genauer reglementiert werden soll (Schulungsraum einer Firma, Schülernetzwerk in einer Schule).

- **hohes Vertrauen:**
  Schnittstellen mit dieser Einstellung belegen die daran angeschlossenen Netzwerke mit den geringsten Einschränkungen. Üblicherweise wird die Schnittstelle zum internen Netzwerk auf diesen Wert eingestellt.

Eine Übersicht, wie mit IP-Paketen bei den jeweiligen Vertrauensstufen (VS) verfahren wird, soll die folgende Tabelle vermitteln:

Pakete von	Pakete nach				
	VS keines	VS gering	VS mittel	VS hoch	DEFENDO
VS keines					
VS gering					
VS mittel	NAT				
VS hoch	NAT				
DEFENDO					

	Zugriff gesperrt, kann definiert freigegeben werden
	Zugriff frei, kann jedoch auf definierte Regeln beschränkt werden
	Zugriff frei

In den folgenden Masken haben Sie die Möglichkeit mit der Angabe von Protokoll, IP-Adresse, Netzmaske und Portnummern bestimmte Dienste freizugeben.

Mit Protokoll legen Sie fest, ob sich die Regel auf das TCP-, UDP- oder ICMP-Protokoll bezieht. An manchen Stellen steht zusätzlich ein frei definierbares Feld zur Verfügung. Für Protokolle außer TCP, UDP und ICMP können Sie hier die gewünschte Protokollnummer eintragen. Sie können das Feld auch leer lassen, um die Regel auf alle Protokolle wirken zu lassen. In diesem Falle erscheint in der Regelliste ein Stern als Protokoll.

Eine Auswahl-Liste erlaubt es, zu der neu erstellten Regel eine Überprüfung gegen Denial-of-Service Angriffe zu konfigurieren. Für TCP-Verbindungen wird hier die Anzahl Verbindungen pro Sekunde konfiguriert, die von einer Quell-Adresse aus erstellt werden dürfen. Für alle Protokolle außer TCP wird die Anzahl Pakete pro Sekunde konfiguriert.

Als IP-Adresse und Netzmaske tragen Sie entweder eine Netzwerk-Adresse und eine zugehörige Netzmaske ein, um diese Regel für mehrere aufeinanderfolgende IP-Adressen zu konfigurieren. Um eine Regel für genau eine IP-Adresse einzutragen, lassen Sie das Netzmasken Feld frei oder tragen Sie als Netzmaske 255.255.255.255 ein. Wenn Sie weder eine IP-Adresse noch eine Netzmaske eingeben, gilt die Regel für alle IP-Adressen. In der Regelliste erscheint in diesem Falle als IP-Adresse ein Stern.

Der Port spezifiziert den jeweiligen TCP- bzw. UDP-Port für den die Regel gilt. Geben Sie die entsprechende Port-Nummer ein, auf die sich die Regel bezieht. Um einen fortlaufenden Bereich von Ports anzugeben, tragen Sie bitte den ersten und den letzten Port getrennt von einem Doppelpunkt ein (z.B. 1024:65535 um alle anonymen Ports zu adressieren). Einige wenige häufig benötigte Ports können auch mit Ihrem symbolischen Namen in Kleinbuchstaben angegeben werden (z.B. smtp, ftp, pop-3, nntp). Wird kein Port angegeben, so bezieht sich die Regel auf alle Ports. In der Regelliste erscheint als Portnummer ein Stern.

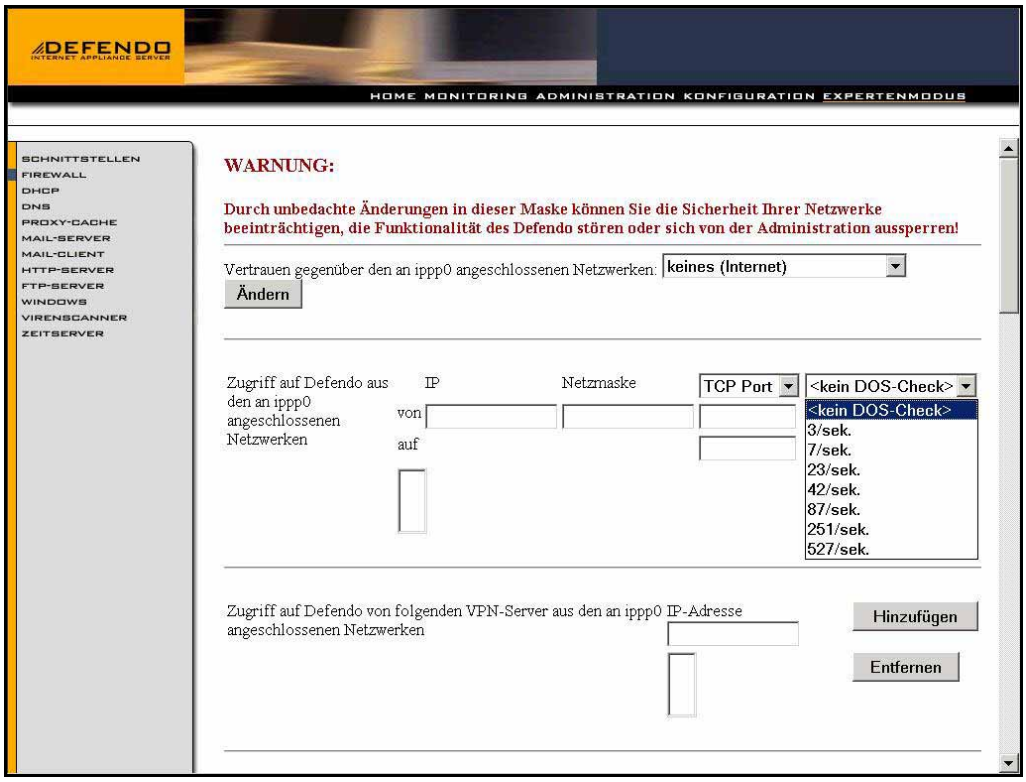
12.2.2.1. Vertrauen nicht definiert – Schnittstelle blockiert

Nach dem Anlegen einer Schnittstelle ist diese zunächst blockiert. Alle IP-Pakete die über diese Schnittstelle laufen werden abgewiesen. Wählen Sie eine passende Vertrauensstellung aus und drücken Sie auf Ändern um die Schnittstelle freizugeben. Die Schnittstelle verhält sich danach so, wie in der Übersichtstabelle dargestellt.

12.2.2.2. Vertrauen keines (Internet)

Vertrauen gegenüber den an ... angeschlossenen Netzwerken

Um die Vertrauensstellung der Schnittstelle zu ändern, wählen Sie bitte die gewünschte Stufe aus der Auswahlliste aus und drücken Sie auf Ändern.



Zugriff auf DEFENDO aus den an ... angeschlossenen Netzwerken

Um eine neue Regel hinzuzufügen, wählen Sie bitte zunächst das gewünschte Protokoll aus. Aktivieren Sie die Denial-of-Service Überwachung falls dies für die neue Regel gewünscht ist. Tragen Sie in der von-Zeile die erforderlichen Werte ein falls Sie die Absender-Adressen und / oder Absender-Ports filtern wollen. Lassen Sie die von-Zeile frei, wenn die Absender-Daten beliebig sein sollen. Tragen Sie in der auf-Zeile den Port des DEFENDO ein, auf den der Zugriff freigegeben werden soll.

Achtung:

Wenn Sie dieses Feld frei lassen, erteilen Sie dieser Schnittstelle Zugriff auf alle Dienste des DEFENDOs!

Drücken Sie nun auf Hinzufügen um die Regel zu aktivieren.

Eingetragene Regeln erscheinen in der Liste im Format

Protokoll:*Quelladresse*(*Quellport*)->IP(*Zielport*){*DOS*}

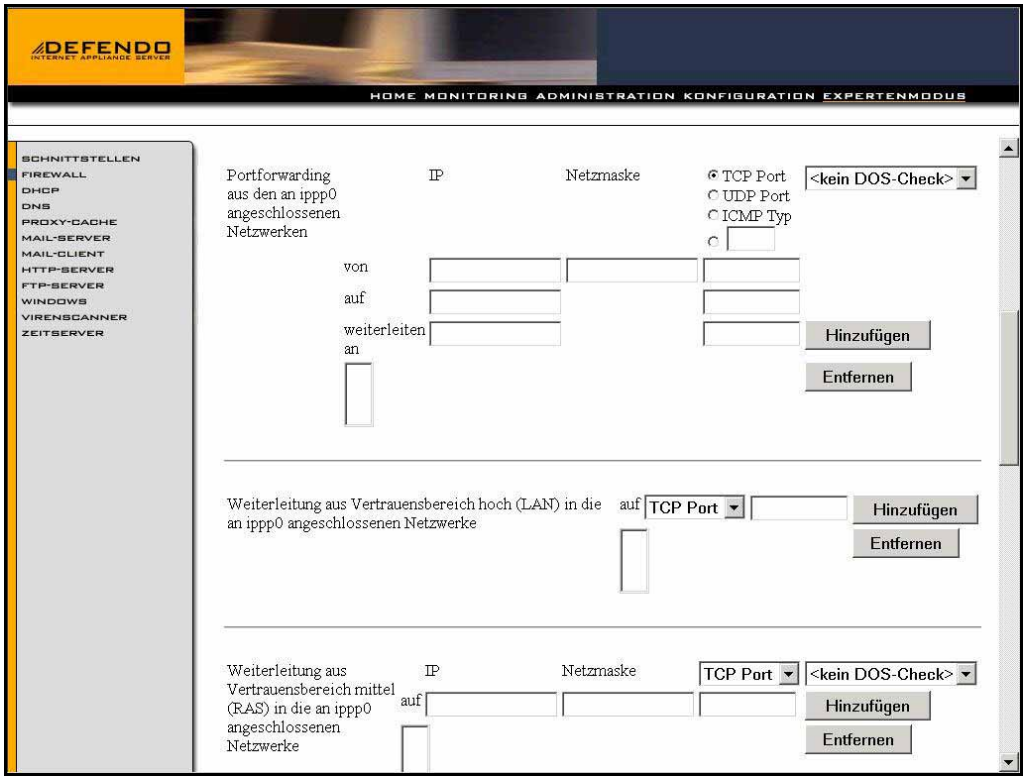
Um eine Regel zu löschen, wählen Sie diese bitte aus der Liste aus und drücken Sie auf Entfernen.

Zugriff auf DEFENDO von folgenden VPN-Servern aus den an ... angeschlossenen Netzwerken

Um die Kommunikation eines VPN-Servers mit dem VPN-Server des DEFENDO zu ermöglichen, müssen Sie hier die IP-Adressen der VPN-Server hinterlegen, die Zugriff erhalten soll. Von den hier angegebenen Adressen werden sowohl UDP-Pakete mit Quell- und Zielport 500 (Internet Key Exchange) akzeptiert als auch alle Pakete der VPN-Protokolle AH und ESP.

Um einen neuen VPN-Server hinzuzufügen tragen Sie dessen IP-Adresse ein. Um den Zugriff von VPN-Servern mit dynamischer IP-Adresse zu erlauben geben Sie bitte als IP-Adresse 0.0.0.0 ein. Drücken Sie auf Hinzufügen um die Regel zu aktivieren.

Um einen VPN-Server zu löschen, wählen Sie ihn aus der Liste aus und drücken Sie auf Entfernen.



Portforwarding aus den an ... angeschlossenen Netzwerken

Beim Portforwarding (DNAT) werden die Zieladressen der IP-Header im DEFENDO manipuliert, um eine definierte Umlenkung eines Datenstroms in einen geschützten Netzwerk-Bereich zu ermöglichen. Von außen erscheint es so, als ob die Kommunikation mit einem Dienst auf dem DEFENDO oder einem anderen System abgewickelt wird. Erreichen die IP-Pakete den DEFENDO, so werden jedoch deren Zieladresse und auf Wunsch auch deren Zielport verändert und so an einen anderen Empfänger weitergeleitet. Bei Antwortpaketen werden diese Änderungen entsprechend rückgängig gemacht. Ein Beispiel: Die IP-Adresse des DEFENDO zum Internet hin sei die 1.1.1.1. Die Rechner im LAN verfügen über keine im Internet gültigen IP-Adressen, trotzdem soll der POP3-Server mit der IP-Adresse 192.168.0.1 vom Internet aus erreichbar sein. Es wird nun eine Portforwarding-Regel eingetragen, die Zugriffe auf den POP3-Port 110 der IP 1.1.1.1 weiterleitet an die Adresse 192.168.0.1, Port 110. Erreicht nun ein IP-Paket mit der Zieladresse 1.1.1.1 und dem Zielport 110 den DEFENDO, so wird die Empfängeradresse auf 192.168.0.1 verändert. Der Zielport bleibt in diesem Beispiel unverändert. Das Paket wird nun an den internen POP3-Server weitergeleitet. Ein Zugriff auf den POP3-Server des DEFENDO ist über die IP-Adresse 1.1.1.1 nicht mehr möglich (wohl aber über andere IP-Adressen des DEFENDO). Soll unter Verwendung der gleichen externen IP-Adresse sowohl der Zugriff auf den POP3-Server des

DEFENDO als auch auf den interner POP3-Server möglich sein, so muß das Portforwarding auf einen anderen Port reagieren. So muß dann z.B. der DEFENDO-Port 109 auf die 192.168.0.1 Port 110 weitergeleitet werden. Der POP3-Client mit dem der Zugriff aus dem Internet erfolgen soll, muß entsprechend auf einen anderen Port als den Standard-Port 110 konfigurierbar sein. Alles was nun hier exemplarisch für das POP3-Protokoll erläutert wurde läßt sich entsprechend auf andere Protokolle übertragen.

Um eine neue Portforwarding-Regel hinzuzufügen wählen Sie bitte zunächst das gewünschte Protokoll aus. Aktivieren Sie wenn gewünscht die Denial-of-Service Überwachung. In der von-Zeile können Sie wenn gewünscht die Absender-Adresse und / oder den Absender-Port filtern. In der Zeile „auf“ können Sie die IP-Adresse und den Zielport angeben, auf die die Portforwarding-Regel reagieren soll. Wenn Sie das IP-Adress-Feld frei lassen, wird die Regel bei jedem passenden eingehenden Paket aktiv, unabhängig von der angesprochenen Ziel-IP-Adresse. Dies ist insbesondere dann sinnvoll, wenn der DEFENDO selbst eine dynamische IP-Adresse hat. Unabhängig davon spielt es jedoch keine Rolle, ob es sich bei der angesprochenen Ziel-Adresse um eine IP-Adresse des DEFENDO handelt oder um eine Adresse eines anderen Systems. Entscheidend ist lediglich, dass das eingehende Paket über die aktuelle Schnittstelle empfangen wird. Auch das Port-Feld darf leer bleiben. Die Regel findet in diesem Falle bei jedem angesprochenen Port anwendung. Bei „weiterleiten an“ ist schließlich die Ziel-IP-Adresse sowie der Ziel-Port anzugegeben. Die Ziel-IP muß dabei angegeben werden. Wird kein Ziel-Port angegeben, so bleibt der Zielport des Original-Paketes unverändert. Die Angabe eine Port-Bereiches oder symbolischer Port-Namen ist hier unzulässig. Drücken Sie dann auf Hinzufügen.

Portforwarding-Regeln werden in folgendem Format angezeigt:

Protokoll:*Quelladresse*(*Quellport*)->*Zieladresse*(*Zielport*)->*interne Adresse*(*interner Port*){*DOS*}

Um eine Regel zu löschen wählen Sie diese bitte aus der Liste aus und drücken Sie auf Löschen.

Weiterleitung aus Vertrauensbereich hoch (LAN) in die an ... angeschlossenen Netzwerke

Die Weiterleitung von Paketen aus dem Vertrauensbereich hoch ist standardmäßig gesperrt. Die am häufigsten benötigte Kommunikation wie Surfen oder Mail sollte über den Proxy-Cache und den SMTP- bzw. POP3/IMAP4-Server des DEFENDO abgewickelt werden. Ist dies nicht ausreichend, so kann über diesen bewußt einfach gehaltenen Masken-

bereich definiert der direkte Zugriff in das Internet freigegeben werden. Dabei kommt die Network-Adress-Translation (NAT, SNAT, masquerading) zum Einsatz. Bei ausgehenden Paketen wird die Absender-Adresse durch die IP-Adresse des DEFENDO ersetzt. Um die Verbindung eindeutig zu halten wird bei Bedarf zusätzlich der Absender-Port geändert. Nach außen hin versteckt sich somit der eigentliche Absender hinter der IP-Adresse des DEFENDO . Bei Antwort-Paketen wird die Änderung wieder rückgängig gemacht. Spezielle Regeln für Antwortpakete müssen dabei nicht konfiguriert werden.

Um einen Dienst freizugeben wählen Sie bitte zunächst das Protokoll aus. Tragen Sie dann die Port-Nummer oder den Port-Bereich ein.

Achtung:

Wenn Sie keinen Port eintragen werden alle Ports zur Weiterleitung freigegeben!

Drücken Sie dann auf Hinzufügen.

Ein Hinweis zum FTP-Protokoll: Der Datei-Download mit Hilfe eines Web-Browsers ist über den Proxy-Cache des DEFENDO möglich. Für den FTP-Upload (z.B. zur Pflege von externen Web-Seiten) ist ein normales FTP-Programm auf den Clients im LAN erforderlich. Ein Proxy darf im FTP-Programm nicht konfiguriert werden. Um den FTP-Zugriff für FTP-Programme freizuschalten, genügt es den FTP-Kontroll-Port als Regel einzutragen. Wählen Sie hierzu das Protokoll TCP und tragen Sie als Port den symbolischen Namen ftp oder die Portnummer 21 ein. Wählen Sie dann Hinzufügen. Es stehen damit automatisch der aktive und der passive FTP-Übertragungsmodus zur Verfügung.

Die Regeln werden in folgendem Format angezeigt:

Protokoll:NET(*)->*(*Zielport*)

Um eine Regel zu löschen wählen Sie diese bitte aus und drücken Sie auf Entfernen.

Wenn Sie eine Weiterleitung genauer definieren wollen (z.B. nur für bestimmte Absenderadressen oder nur auf einen bestimmten Zielserver), benutzen Sie bitte die „Benutzerdefinierten Weiterleitungen“ am Ende der Maske. Vergessen Sie dabei nicht, NAT zu aktivieren.

Weiterleitung aus Vertrauensbereich mittel (RAS) in die an ... angeschlossenen Netzwerke

Diese Maske ist identisch mit der zuvor beschriebenen Weiterleitung aus Vertrauensbereich hoch mit folgenden Unterschieden:

Es läßt sich auf Wunsch auch Denial-of-Service Überwachung sowie die Ziel-IP-Adresse bzw. das Ziel-Netzwerk angeben. Die Anzeige erfolgt im Format

Protokoll:NET(*)->*Zieladresse*(*Zielport*){*DOS*}

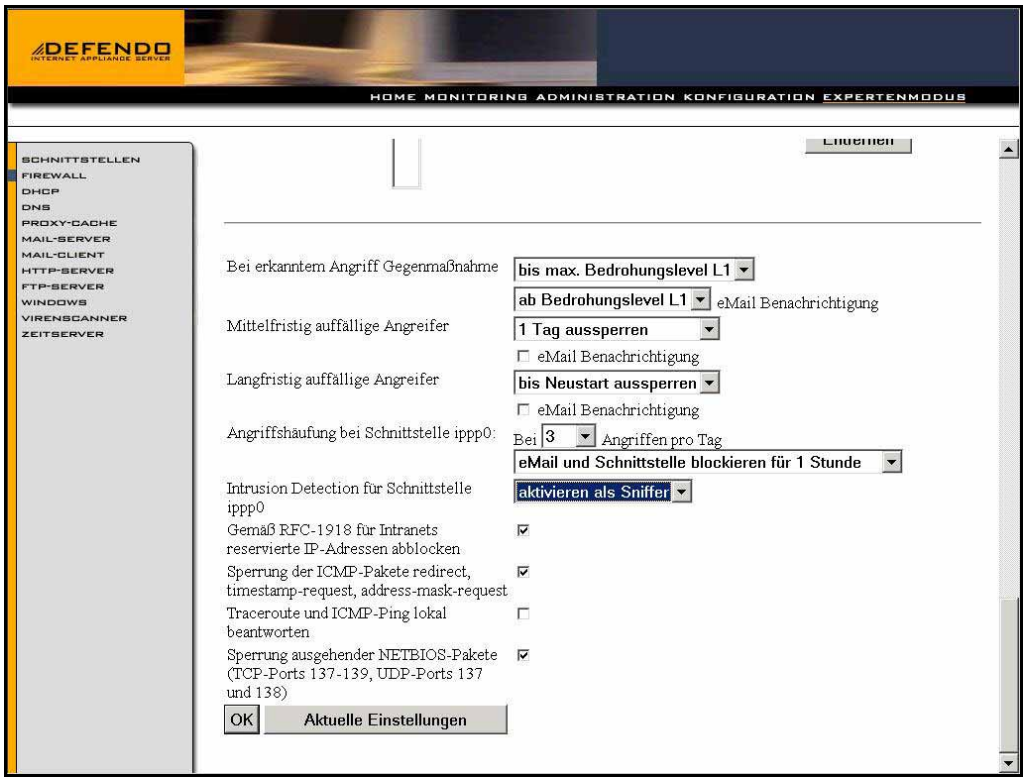
Weiterleitung aus Vertrauensbereich keines (Internet) in die an ... angeschlossenen Netzwerke

Auf Wunsch kann Denial-of-Service Überwachung aktiviert werden. Wählen Sie das Protokoll und tragen Sie die Filterregeln für Quell- und Zieldaten ein um zwischen zwei Schnittstellen mit Vertrauensstellung keines zu routen. Dieser Fall dürfte in der Praxis eher selten auftreten.

Drücken Sie auf Hinzufügen um eine Regel zu konfigurieren. Die Anzeige erfolgt im Format

Protokoll:*Quelladresse*(*Quellport*)->*Zieladresse*(*Zielport*){*DOS*}

Wählen Sie eine Regel aus der Liste und drücken Sie auf Entfernen um die Regel zu löschen.



Benutzerdefiniert Weiterleitung in die an ... angeschlossenen Netzwerke

Hier können Sie Weiterleitungen an die aktuelle Schnittstelle frei definieren. Aktivieren Sie Denial-of-Service Überwachung wenn gewünscht. Wählen Sie das Protokoll und tragen Sie die passenden Werte für Quelle und Ziel ein. Wenn gewünscht oder erforderlich aktivieren Sie zusätzlich Network-Adress-Translation (NAT, SNAT, masquerading). Lassen Sie das Eingabefeld für die IP-Adresse leer, wenn das System die NAT-Adresse selbständig bestimmen darf. Tragen Sie hier eine Adresse ein, um zu dieser Regel immer eine feste NAT-Adresse zu verwenden. Die NAT-Adresse sollte in diesem Falle natürlich eine Adresse des DEFENDO selbst sein. Obwohl die Regel im Weiterleitungsbereich eingetragen wird, kann mit Hilfe einer Regel in diesem Bereich NAT auch auf IP-Pakete angewendet werden, die vom DEFENDO selbst stammen.

Drücken Sie auf Hinzufügen um die Regel zu aktivieren. Die Anzeige erfolgt in folgendem Format wenn NAT für die entsprechende Regel nicht aktiv ist:

Protokoll:*Quelladresse*(*Quellport*)->*Zieladresse*(*Zielport*){*DOS*}

bzw. bei aktivierter NAT:

Protokoll:*Quelladr.*(*Quellport*)->*Zieladr.*(*Zielport*)[NAT:*NAT-IP*]{*DOS*}

Wählen Sie eine Regel aus der Liste und drücken Sie auf Entfernen um die Regel zu löschen.

Bei erkanntem Angriff Gegenmaßnahme

In der Firewall-Hauptmaske haben Sie konfiguriert, welche Maßnahme vom dynamischen Firewall gegen eine IP-Adresse eingeleitet werden soll, wenn diese den Schwellwert eines bestimmten Bedrohungslevels erreicht. Über diesen Schalter können Sie nun bestimmten, wie weit diese Schwellwerte in dieser Schnittstelle überhaupt beachtet werden sollen. So mag es für eine Internet-Schnittstelle in Ordnung sein, eine IP-Adresse bis zum nächsten Neustart auszusperren, während dies für eine LAN-Schnittstelle nicht unbedingt gewünscht ist. Ferner können Sie hier einstellen, ab welchem Level der admin per Mail über IP-Adressen informiert werden soll, gegen die eine Gegenmaßnahme eingeleitet wurde. Für Bedrohungslevel bei denen keine Gegenmaßnahme eingeleitet wird, wird auch keine eMail versendet.

Mittelfristig / Langfristig auffällige Angreifer

Werden von einer Adresse mittelfristig (< 24h) oder langfristig immer wieder verdächtige Pakete gemeldet, kann hier die Gegenmaßnahme aktiviert werden. Auf Wunsch wird eine Benachrichtigungsmail an den admin gesendet. Hier ist auch eine Benachrichtigung möglich, wenn keine Gegenmaßnahme eingeleitet wird.

Angriffshäufung bei Schnittstelle ...

Hier wird adressübergreifend die Summe aller Gegenmaßnahmen betrachtet. Wird der hier konfigurierten Wert erreicht, so wird die eingestellte Maßnahme ergriffen. Um diesen Wert sinnvoll zu konfigurieren, ermitteln Sie zunächst über einige Tage die für Ihre Internetanbindung „normalen“ Wert an Angriffen pro Tag. Konfigurieren Sie dann einen höheren Wert, um ungewöhnlich viele Angriffe von verschiedenen IP-Adressen zu erkennen.

Intrusion-Detection für Schnittstelle ...

Sofern das Intrusion-Detection-System aktiviert ist, können Sie hier angeben, ob bzw. wie die aktuelle Schnittstelle überwacht werden soll: Bei „deaktiviert“ werden keine Pakete an die Intrusion-Detection übermittelt. Bei der Einstellung „aktiviert“ werden alle Pakete die die Schnittstelle passieren überwacht. Ist die Intrusion-Detection „aktiviert als sniffer“ werden zusätzlich alle Pakete überwacht die an der Netzwerkkarte physikalisch anliegen. Ist die entsprechende Schnittstelle z.B. an einem Hub angeschlossen, so wird die gesamte Kommunikation die über diesen Hub abgewickelt wird an die Intrusion-Detection weitergegeben.

Gemäß RFC-1918 für Intranets reservierte IP-Adressen abblocken

Bei aktiviertem Schalter werden alle Pakete die über diese Schnittstelle laufen auf IP-Adressen aus den Netzwerken 192.168.0.0/255.255.0.0, 172.16.0.0/255.240.0.0 und 10.0.0.0/255.0.0.0 überprüft. Alle eingehenden und ausgehenden Pakete mit entsprechender Absender- oder Empfänger-Adresse werden blockiert. Drücken Sie auf „OK“ am Ende der Maske um diese Einstellung zu aktivieren.

Sperrung der ICMP-Pakete redirect, timestamp-request, address-mask-request

Bei aktiviertem Schalter werden die genannte ICMP-Pakettypen bei eingehenden Paketen blockiert. Drücken Sie auf „OK“ am Ende der Maske um diese Einstellung zu aktivieren.

Traceroute und ICMP-Ping lokal beantworten

Eingehende ICMP echo-request-Pakete werden unabhängig von der eigentlichen Ziel-Adresse vom Firewall selbst mit einem echo-reply be-

antwortet. Eingehende Pakete mit ttl Wert-1 gefolgt von Paketen mit ttl-Wert 2 deuten auf einen Traceroute hin. Diese werden ebenfalls unabhängig von der eigentlichen Ziel-Adresse vom DEFENDO beantwortet, so dass es für den Absender des traceroutes so aussieht, als ob er im DEFENDO das Ziel-System erreicht hat. Wird der DEFENDO vor einem Netzwerk mit Internet-Adressen betrieben (z.B. vor einer DMZ), so kann deren Struktur und die tatsächlich aktiven Rechner weitgehend verborgen werden.

Sperrung ausgehender NETBIOS-Pakete

Ist dieser Schalter aktiv, werden ausgehende Pakete an die Microsoft NETBIOS-Ports 137-139 (TCP) und 137-138 (UDP) blockiert. Diese Einstellung empfiehlt sich insbesondere bei der Internetanbindung über Wählleitung, um unnötige Kosten verursacht durch das recht „geschwätzige“ NETBIOS-Protokoll zu verhindern. Drücken Sie auf „OK“ am Ende der Maske um diese Einstellung zu aktivieren.

12.2.2.3. Vertrauen gering (Demilitarisierte Zone)

Vertrauen gegenüber den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Zugriff auf DEFENDO aus den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Zugriff auf DEFENDO von folgenden VPN-Servern aus den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Portforwarding aus den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Weiterleitung aus Vertrauensbereich mittel (RAS) in die an ... angeschlossenen Netzwerke

Wählen Sie zunächst das gewünschte Protokoll aus. Auf Wunsch kann die Denial-of-Service Überwachung aktiviert werden. Tragen Sie dann die gewünschten Ziel-Adressen und –Ports ein. Drücken Sie auf Hinzufügen um die Regel zu aktivieren.

Die Anzeige der Regeln erfolgt im Format

Protokoll:NET(*)->*Zieladresse*(*Zielport*){*DOS*}

Um eine Regel zu löschen, wählen Sie diese aus der Liste aus und drücken Sie auf Entfernen.

Weiterleitung aus Vertrauensbereich keines (Internet) in die an ... angeschlossenen Netzwerke

Wählen Sie zunächst das gewünschte Protokoll aus. Aktivieren Sie bei bedarf die Denial-of-Service Überwachung. Tragen Sie dann die gewünschten Quell- und Zieldaten ein. Drücken Sie auf Hinzufügen um die Regel zu aktivieren.

Die Anzeige der Regeln erfolgt im Format

Protokoll:*Quelladresse*(*Quellport*)->*Zieladresse*(*Zielport*){*DOS*}

Um eine Regel zu löschen, wählen Sie diese aus der Liste aus und drücken Sie auf Entfernen.

Benutzerdefinierte Weiterleitung in die an ... angeschlossenen Netzwerke

Siehe Vertrauen keines (Internet)

Zugriff von DEFENDO in die an ... angeschlossenen Netzwerke

Mit Hilfe dieser Einstellung lassen sich TCP-Zugriffe vom DEFENDO aus in die entsprechenden Netzwerke verhindern. In der von-Zeile können Sie den Quell-Port auf Seiten des DEFENDO filtern. In der auf-Zeile können Sie nach Bedarf die Ziel-Adressen und / oder Ziel-Ports filtern. Auf Wunsch zusätzlich mit Denial-of-Service Überwachung. Benutzen Sie diese Einstellung um zu verhindern, daß Sicherheitsregeln die bezüglich der direkten Weiterleitung definiert wurden nicht mit Hilfe von Diensten unterlaufen werden, die auf dem DEFENDO selbst aktiv sind (z.B. läßt sich unter Umständen mit Hilfe des Proxy-Caches des DEFENDO auf einen Dienst zuzugreifen, zu dem eine direkte Durchleitung gesperrt ist).

Drücken Sie auf Hinzufügen um eine neue Regel zu aktivieren. Die Regeln werden in folgendem Format dargestellt:

Protokoll:IP(*Quellport*)->*Zieladresse*(*Zielport*){*DOS*}

Um eine Regel zu löschen wählen Sie diese aus der Liste aus und drücken Sie auf Entfernen.

Bei erkanntem Angriff Gegenmaßnahme

Siehe Vertrauen keines (Internet)

Mittelfristig / Langfristig auffällige Angreifer

Siehe Vertrauen keines (Internet)

Angriffshäufung bei Schnittstelle ...

Siehe Vertrauen keines (Internet)

Intrusion-Detection für Schnittstelle ...

Siehe Vertrauen keines (Internet)

Gemäß RFC-1918 für Intranets reservierte IP-Adressen abblocken

Siehe Vertrauen keines (Internet)

Sperrung der ICMP-Pakete redirect, timestamp-request, address-mask-request

Siehe Vertrauen keines (Internet)

Traceroute und ICMP-Ping lokal beantworten

Siehe Vertrauen keines (Internet)

Sperrung ausgehender NETBIOS-Pakete

Siehe Vertrauen keines (Internet)

12.2.2.4. Vertrauen mittel (RAS)

Vertrauen gegenüber den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Zugriff auf DEFENDO aus den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Zugriff auf DEFENDO von folgenden VPN-Servern aus den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Weiterleitung aus Vertrauensbereich mittel (RAS) in die an ... angeschlossenen Netzwerke

Siehe Vertrauen gering (Demilitarisierte Zone)

Benutzerdefinierte Weiterleitung in die an ... angeschlossenen Netzwerke

Siehe Vertrauen keines (Internet)

Zugriff von DEFENDO in die an ... angeschlossenen Netzwerke

Siehe Vertrauen gering (Demilitarisierte Zone)

Bei erkanntem Angriff Gegenmaßnahme

Siehe Vertrauen keines (Internet)

Mittelfristig / Langfristig auffällige Angreifer

Siehe Vertrauen keines (Internet)

Angriffshäufung bei Schnittstelle ...

Siehe Vertrauen keines (Internet)

Intrusion-Detection für Schnittstelle ...

Siehe Vertrauen keines (Internet)

12.2.2.5. Vertrauen hoch (LAN)

Vertrauen gegenüber den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Zugriff auf DEFENDO von folgenden VPN-Servern aus den an ... angeschlossenen Netzwerken

Siehe Vertrauen keines (Internet)

Weiterleitung aus Vertrauensbereich mittel (RAS) in die an ... angeschlossenen Netzwerke

Siehe Vertrauen gering (Demilitarisierte Zone)

Benutzerdefinierte Weiterleitung in die an ... angeschlossenen Netzwerke

Siehe Vertrauen keines (Internet)

Zugriff von DEFENDO in die an ... angeschlossenen Netzwerke

Siehe Vertrauen gering (Demilitarisierte Zone)

Bei erkanntem Angriff Gegenmaßnahme

Siehe Vertrauen keines (Internet)

Mittelfristig / Langfristig auffällige Angreifer

Siehe Vertrauen keines (Internet)

Angriffshäufung bei Schnittstelle ...

Siehe Vertrauen keines (Internet)

Intrusion-Detection für Schnittstelle ...

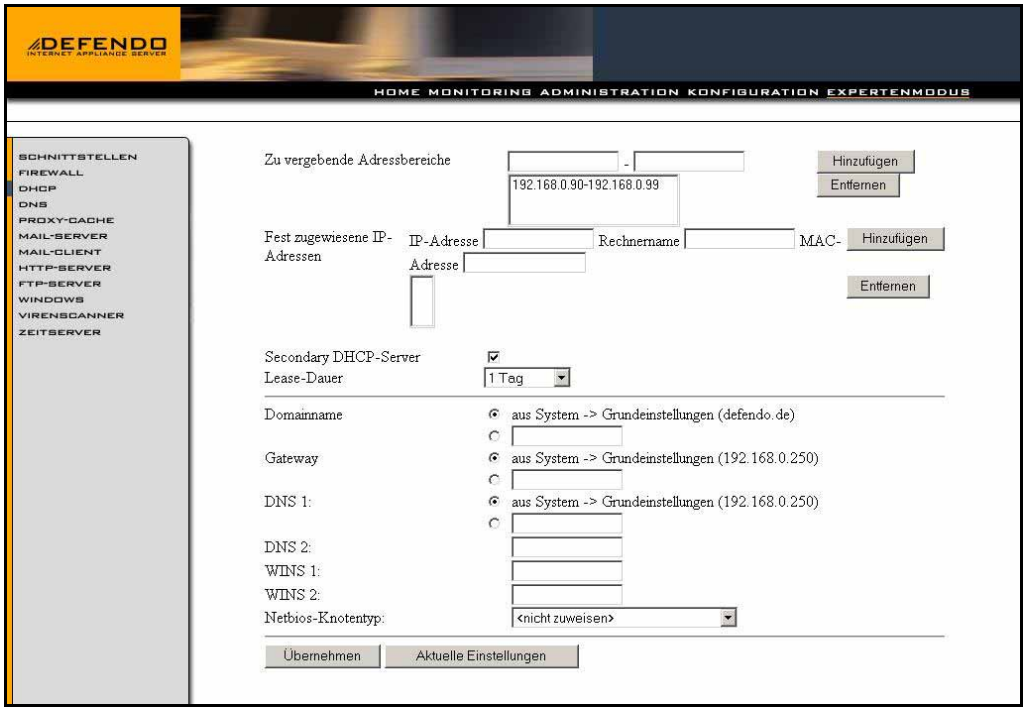
Siehe Vertrauen keines (Internet)

12.2.2.6. Vertrauen Fernwartung

Diese Vertrauenseinstellung ist fest im System hinterlegt und kann nicht geändert werden. Ausschließlich der verschlüsselte Zugriff zwischen DEFENDO und Support-Server sowie das ICMP-Protokoll sind hier freigeschaltet.

12.3. DHCP

Dieses Modul dient zur Konfiguration der DHCP-Funktion des DEFENDO. Da diese Funktion schon mit dem Konfigurations-Assistenten „LAN-Anbindung“ eingestellt wird (wenn dies gewünscht wurde), sind hier eventuell schon Eintragungen vorhanden. Sie können diese hier verändern bzw. ergänzen oder komplett neu einrichten.



Im Eingabefeld „Zu vergebender Adressbereiche“ muß die Start- und End-Adresse des Bereiches eingetragen werden, die der DEFENDO dynamisch an anfragende Geräte vergeben soll. Es können natürlich mehrere Adressbereiche definiert werden.

> *Hinweis:*
>
> *Bitte beachten Sie bei der Vergabe von Adressbereichen, dass keine Bereiche definiert werden, in denen bereits feste IP-Adressen zum Einsatz kommen, da es sonst zu Konflikten mit doppelten IP-Adressen kommen kann!*

Sie können ferner fest zugewiesene IP-Adressen vergeben um zu gewährleisten, dass ein bestimmtes Gerät im Netzwerk immer unter der gleichen IP-Adresse erreichbar ist. Das Gerät wird dabei an der Hardware-Adresse von dessen Netzwerkkarte (MAC-Adresse) identifiziert. Um einem Gerät eine feste Adresse zuzuweisen, geben Sie bitte in den zugehörigen Feldern die gewünschte IP-Adresse, einen Namen sowie die das Gerät identifizierende MAC-Adresse ein. Die IP-Adresse sollte dabei nicht in den dynamisch zu vergebenden IP-Adressbereichen enthalten sein. Die MAC-Adresse ist in hexadezimaler Schreibweise anzugeben, die einzelnen Bytes mit Doppelpunkten getrennt (z.B. 0a:43:94:fc:83:0e). Drücken Sie „Hinzufügen“ um die statische Adresszuweisung zu aktivieren. Wählen Sie eine bereits angelegte statische

Adresszuweisung aus der Liste und drücken Sie auf „Entfernen“ um diese Zuweisung aufzuheben.

Wählen Sie den Optionshaken bei „Secondary DHCP-Server“, wenn Sie wollen, dass der DEFENDO nur IP-Adressen an Geräte vergibt, wenn diese Ihre Anfrage nach einer IP-Adresse wiederholt stellen. Dies ist dann hilfreich, wenn ein anderer Server in Ihrem Netz bereits die Funktion des DHCP-Servers übernommen hat und nicht zur Verfügung steht oder ausgefallen ist. Bitte beachten Sie, dass die IP-Adressbereiche die der primäre und der sekundäre DHCP-Server dynamisch vergeben sich nicht überschneiden dürfen. Schließlich ist dem primären DHCP-Server die existenz eines sekundären Servers nicht bewusst, so dass es bei Überschneidungen zu Konflikten kommen kann.

Mit Hilfe der Lease-Dauer können Sie bestimmen, wie lange eine zugewiesene Adresse für ein Gerät reserviert bleiben soll. Setzen Sie diese Adresse auf einen niedrigen Wert, wenn häufig Geräte nur kurz in das LAN eingebunden werden.

Domainname, Gateway und DNS1 beziehen sich in der Regel immer auf Ihren DEFENDO . Deswegen ist in der Grundeinstellung hierfür immer die IP-Adresse des DEFENDO eingetragen. In bestimmten Fällen kann es jedoch notwendig sein diese zu ändern. In diesem Fall wählen Sie bitte den Optionsschalter unterhalb der „Grundeinstellung“ und tragen Ihre gewünschten Angaben ein.

Bei DNS2 haben Sie die Möglichkeit, einen zweiten DNS-Server einzutragen, der dann zum Einsatz kommt, wenn der DNS1 die Anfrage nicht auflösen kann. Dies kann z. B. ein DNS-Server Ihres Providers sein, oder ein DNS-Server innerhalb Ihres LANs. Tragen Sie auch hier die entsprechende IP-Adresse dieses Server ein.

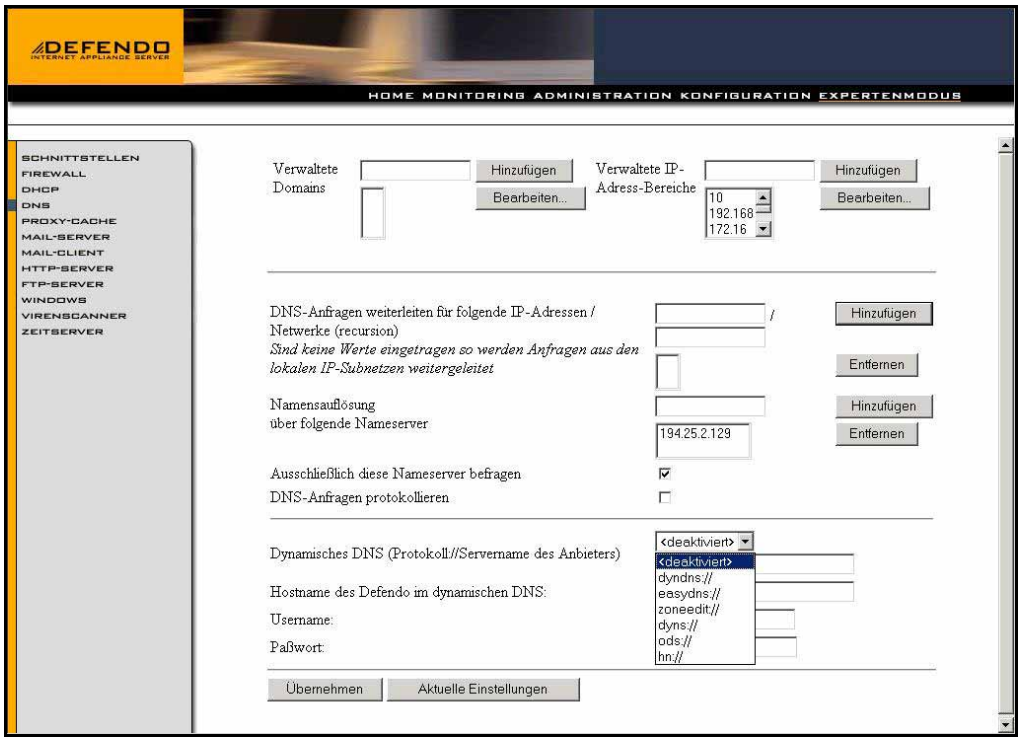
Bei WINS1 und WINS2 können Sie WINS-Server für Microsoft-Windows über DHCP vergeben. Tragen Sie hier die entsprechenden IP-Adressen ein.

Speziell für Microsoft-Windows lässt sich auch der Netbios-Knotentyp zuweisen. Wählen Sie in diesem Falle den passenden Knotentyp aus. Soll keine Zuweisung des Netbios-Knotentyps stattfinden, so wählen Sie bitte „<nicht zuweisen>“.

Zur Übernahme Ihrer Änderungen bestätigen Sie bitte den Schalter „Übernehmen“. Die entsprechenden Dienste des DEFENDO werden nun neu gestartet.

12.4. DNS

Der DEFENDO kann als DNS-Server für mehrer Domains in Ihrem LAN eingesetzt werden. Aber auch die Namensauflösungen über andere DNS-Server wird hier konfiguriert. Zudem können für die eingetragenen Domains Einstellungen (z. B. für Benutzereinträge, Mailexchanger, etc.) gemacht werden.



Im oberen Bereich der Maske werden die Grundeinstellungen des DNS-Servers des DEFENDO angezeigt, d. h. die verwalteten Domains, sowie die IP-Adressbereiche, die durch den DEFENDO verwaltet werden.

Die Weiterleitung von DNS-Anfragen in das Internet (recursion) ist beschränkt auf Anfragen die aus den lokalen IP-Netzwerke gestellt werden. Diese sind in den Grundeinstellungen konfiguriert. Die Berechtigung für rekursive DNS-Anfragen lässt sich über den entsprechenden Eingabebereich jedoch auch frei einstellen. Geben Sie einzelne IP-Adressen oder Netzwerkadressen mit zugehöriger Netzmaske ein und drücken Sie „Hinzufügen“ um selbst zu definieren welche Absenderadressen die Berechtigung erhalten, rekursive DNS-Anfragen zu stellen.

Mit Hilfe des „Entfernen“-Schalters werden diese Berechtigungen wieder entzogen. Ist die List leer sind alle lokalen IP-Netzwerke aus den Grundeinstellungen berechtigt.

DNS-Anfragen die vom DEFENDO selbst nicht beantwortet werden können, werden vom DEFENDO in das Internet weitergeleitet. Dazu sollte der DEFENDO die DNS-Anfrage zunächst an die DNS-Server Ihres Providers weitergeben. Geben Sie dazu im Feld „Namensauflösung über folgende Nameserver“ die IP-Adressen der Provider-Nameserver ein und bestätigen Sie dies über den Schalter „Hinzufügen“. Auch hier können Sie jederzeit einen selektierten Eintrag über „Entfernen“ aus der Liste löschen. Ist der Schalter „Ausschließlich diese Nameserver befragen“ nicht aktiviert, so werden zusätzlich die Internet Root-Nameserver befragt, wenn von den konfigurierten Nameserver keine Antwort empfangen wird. Sollte sich der DEFENDO selbst hinter einer Firewall befinden, so ist es im allgemeinen erforderlich, diese Option zu aktivieren und einen durch die vorgelagerte Firewall bestimmten DNS-Server im DEFENDO-DNS zu konfigurieren. Sind keine Nameserver hinterlegt, erfolgt die Namensauflösung stets mit Hilfe der Root-Nameserver des Internets. Die Namensauflösung nimmt in diesem Falle jedoch meist deutlich mehr Zeit in Anspruch.

Der Schalter „DNS-Anfragen protokollieren“ aktiviert die Aufzeichnung jeder Anfrage an den DNS-Server des DEFENDO. Dies kann insbesondere bei der Internetanbindung über Wählleitung nützlich sein, um fehlerhaft konfigurierte Rechner im LAN aufzuspüren, die mit DNS-Anfragen wiederholt Verbindungsaufbauten in das Internet auslösen.

Ist der DEFENDO über eine Wählleitung mit dynamischer IP-Adresse an das Internet angebunden, so kann er bei jedem Aufbau einer neuen Wählverbindung automatisch den DNS-Eintrag bei einem Anbieter von dynamischem DNS aktualisieren. Auf diese Weise kann der DEFENDO trotz der dynamischen IP-Adresse nahezu immer aus dem Internet unter einem definierten Namen erreicht werden, sofern er online ist. Für die Aktualisierung der Einträge im dynamischen DNS gibt es leider keinen einheitlichen Standard. DEFENDO unterstützt jedoch eine ganze Reihe von Protokollen für diese Aktualisierung. Bitte klären Sie zunächst mit dem Anbieter des dynamischen DNS-Dienstes, welches Protokoll verwendet wird und ob dieses vom DEFENDO unterstützt wird. Um die automatische Aktualisierung des dynamischen DNS Eintrages zu aktivieren, wählen Sie bitte zunächst das passende Protokoll. Mit Auswahl der Option „deaktiviert“ findet zukünftig keine Aktualisierung mehr statt. Geben Sie hinter dem Protokoll geben Sie bitte den Namen des Servers an, der die Aktualisierungsanfragen entgegennimmt. Dieser Server ist nicht immer identisch mit dem Webserver des Anbieters, unter dem Sie die Zugangsdaten beantragt haben. Geben Sie als

„Hostname des DEFENDO im dynamischen DNS“ den vollständigen Namen ein (inkl. Domain), unter dem der DEFENDO im dynamischen DNS erreichbar ist. Schließlich müssen noch der Benutzername und das Passwort angegeben werden, mit dem der Anbieter des dynamischen DNS-Dienstes die Aktualisierungsanfragen authentifiziert.

Hinweis:

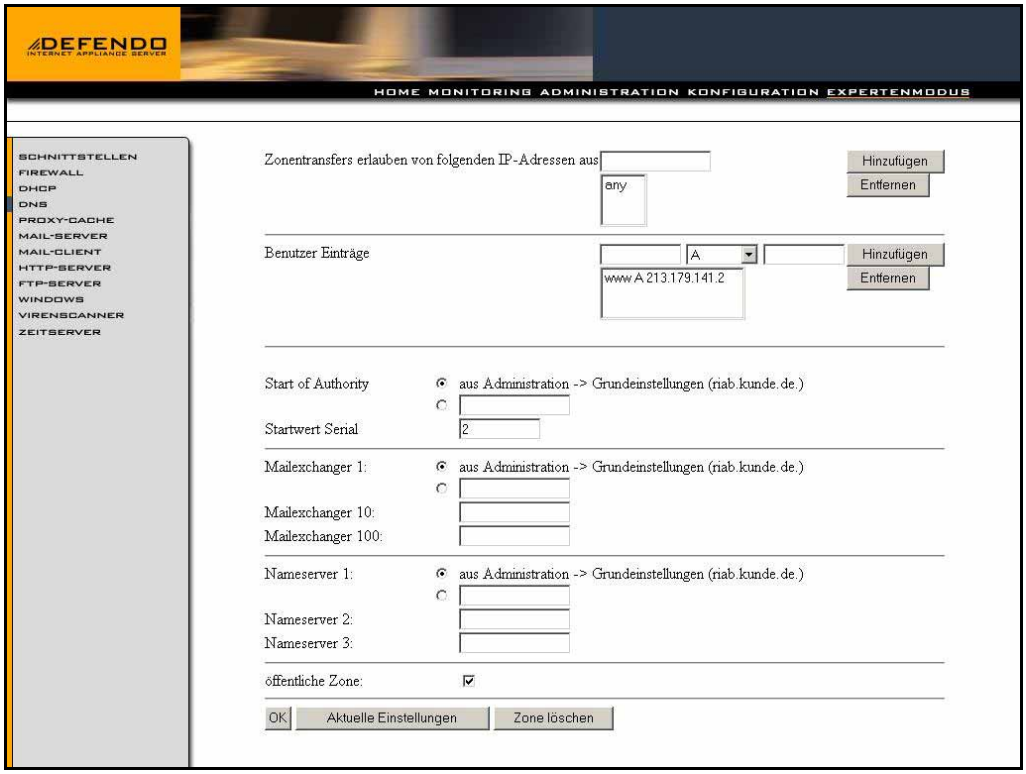
Die Aktualisierung des Eintrages im dynamischen DNS erfolgt einmalig nach jedem Aufbau einer Wählverbindung über die Internet-Schnittstelle (die Schnittstelle, über die aktuell die Default-Route konfiguriert wurde). Danach vergehen einige Sekunden oder Minuten, bis das System auch aus dem Internet unter dem bekannten Namen aber der neuen IP-Adresse erreichbar ist. Nähere Informationen dazu erhalten Sie vom jeweiligen Anbieter des dynamischen DNS-Dienstes.

Eine Aktualisierung kann nur bei ippp- und adsl-Schnittstellen stattfinden.

Wenn eine nahezu permanente Erreichbarkeit gewünscht ist, empfiehlt es sich, bei adsl-Schnittstellen die „niemals trennen“-Option zu aktivieren (vgl. Kapitel 12.1.4).

12.4.1. Verwaltete Domains

Tragen Sie bei Bedarf die gewünschte Domain in das freie Feld ein und bestätigen Sie diese über den Schalter „Hinzufügen“. Ihr neuer Eintrag wird dann in das darunter liegende Listenfeld übernommen. Ist ein Eintrag in diesem Listenfeld selektiert, können Sie über den Schalter „Bearbeiten“ weitere Einstellungen zu dieser Domain vornehmen. Wollen Sie eine Domain aus der Liste löschen, so ist es notwendig, vorher in die Bearbeitungsmaske zu wechseln und mit Hilfe des Schalter „Zone löschen“ diesen Eintrag zu entfernen.



Sie haben hier die Möglichkeit, DNS-Einträge in der verwalteten Domain vorzunehmen.

Zonentransfers erlauben von folgenden IP-Adressen aus

Sofern der DNS-Server des DEFENDO als „offizieller“ DNS-Server im Verbund des Internet-Domain-Name-Services fungiert, müssen die sekundären DNS-Server die DNS-Informationen der verwalteten Domain herunterladen können. Geben Sie hier die IP-Adressen der DNS-Server ein, die berechtigt sind, einen Zonentransfer durchzuführen.

> *Hinweis:*
>
> *Zusätzlich ist im Firewall der TCP-Port 53 freizugeben um Zonentransfers zu ermöglichen.*

Benutzer Einträge

Tragen Sie in das erste Feld bitte den Begriff ein, der im DNS definiert werden soll. Bitte beachten Sie, daß die aktuell verwaltete Zone diesem Begriff angefügt wird, wenn der Begriff nicht mit einem Punkt endet. Ist die aktuelle Zone z.B. domain.com, so steht der Begriff www.domain.com (ohne abschließenden Punkt) tatsächlich für www.domain.com.domain.com. Richtig wäre der Eintrag www oder

www.domain.com. (mit abschließendem Punkt). Wählen Sie dann aus der Liste die Art des Eintrages aus: A um dem Namen eine IP-Adresse zuzuordnen, CNAME um einen Alias-Namen zu spezifizieren, MX um einen Mail-Exchanger mit der entsprechenden Priorität einzutragen und NS um einen DNS-Server zu spezifizieren. In das letzte Feld muß bei Typ A die passende IP-Adresse hinterlegt werden. Bei CNAME, NS und MX ist der zugehörige DNS-Name zu hinterlegen. Auch bei diesen Namen wird automatisch die aktuelle Domain angehängt, wenn kein abschließender Punkt angegeben wird.

Drücken Sie auf Hinzufügen um neue Einträge zu aktivieren. Wählen Sie einen Eintrag aus der Liste aus und drücken Sie auf Entfernen um den Eintrag zu löschen.

Start of Authority

Mit Hilfe dieses Wertes konfigurieren Sie den Hostnamen der im SOA-Record der Domain hinterlegt werden soll. Wählen Sie Grundeinstellung um den aktuellen Hostnamen zu verwenden oder wählen Sie den Optionsschalter vor dem Eingabefeld und geben Sie dort den Hostnamen für den SOA-Record ein.

Startwert Serial

Jede DNS-Zone verfügt über eine fortlaufende Versionsnummer, anhand derer sekundäre DNS-Server entscheiden, ob eine aktueller Version verfügbar und damit ein Zonentransfer notwendig ist. Diese Versionsnummer wird vom DEFENDO automatisch erhöht. Das Eingabefeld „Startwert Serial“ zeigt jeweils den aktuellen Wert an und ermöglicht es diesen zu Verändern.

Mailexchanger

Hier konfigurieren Sie den Mail-Exchanger für die aktuelle Domain. Ist der Mail-Exchanger mit höchster Priorität der DEFENDO selbst, so kann dieser Wert aus den Grundeinstellungen bezogen werden. Wählen Sie den Optionsschalter vor dem Eingabefeld um den Mail-Exchanger mit höchster Priorität selbst zu vergeben. Weitere Mail-Exchanger Einträge können in den folgenden Eingabefeldern mit entsprechender Priorität eingetragen werden.

Nameserver

Hier konfigurieren Sie die Nameserver für die aktuelle Domain. Ist einer der Nameserver der DEFENDO selbst, so kann dieser Wert aus den Grundeinstellungen bezogen werden. Wählen Sie den Optionsschalter vor dem Eingabefeld um einen anderen Wert zu vergeben. Weitere Nameserver-Einträge können in den folgenden Eingabefeldern eingetragen werden.

Öffentliche Zone

DNS-Anfragen an diese Zone sind normalerweise nur aus den lokalen IP-Netzwerken die in den Grundeinstellungen konfiguriert sind erlaubt. Sollen DNS-Anfragen von beliebigen IP-Adressen aus möglich sein, so ist die Zone als „öffentlich“ zu markieren.

> *Hinweis:*
>
> *Um DNS-Anfragen aus dem Internet an den DNS-Server des DEFENDO zu ermöglichen ist je nach Konfiguration. im Firewall zusätzlich der UDP-Port 53 freizugeben.*

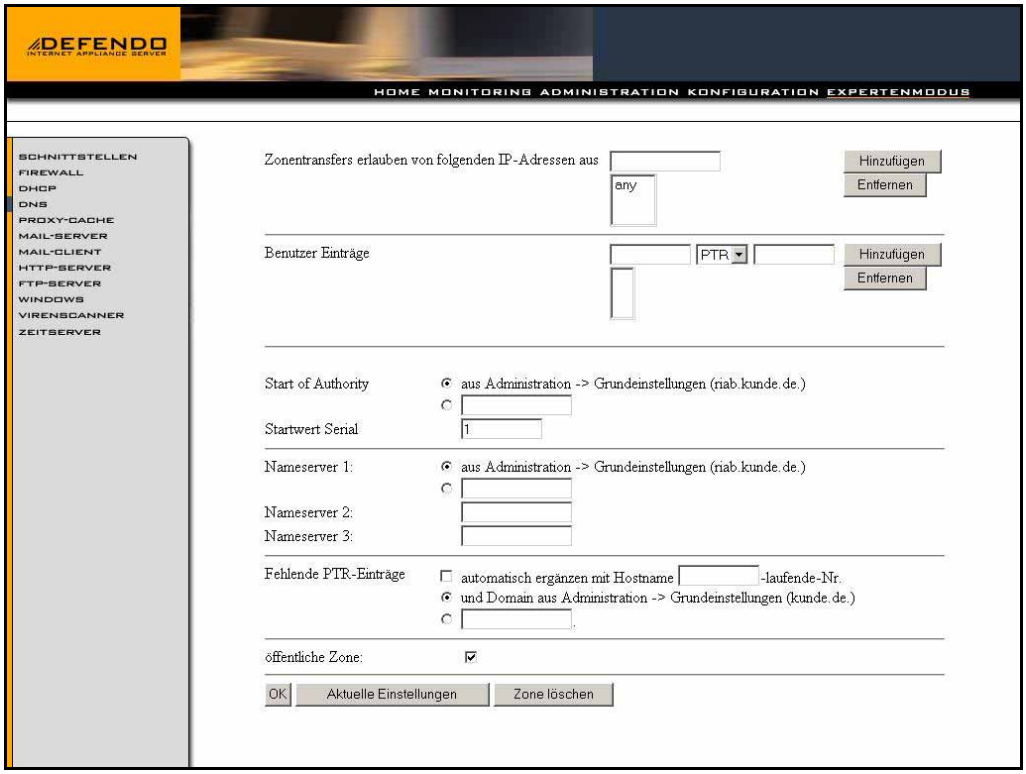
Drücken Sie auf OK um Änderungen zu aktivieren oder wählen Sie Zone löschen um die gesamte DNS-Zone mitsamt aller Einträge zu löschen.

12.4.2. Verwaltete IP-Adressbereiche

Hier wird angegeben, für welche Adressbereiche der DEFENDO zuständig sein soll.

> *Hinweis:*
>
> *Bei einem Eintrag eines Adressbereiches ist es notwendig, nur so viele Stellen der IP-Adresse anzugeben, wie in der dazugehörigen Netzmaske den Wert 255 besitzen (z. B. bei einer Netzwerkadresse 10.1.1.0 und der Netzmaske 255.255.240.0 wäre dies die 10.1).*

Machen Sie Eingabe für einen neuen Adressbereich im Feld „verwaltete IP-Adress-Bereiche“ und bestätigen Sie diese über den Schalter „Hinzufügen“. Im darunter liegenden Listenfeld wird Ihr neuer Eintrag aufgenommen. Weitere Einstellungen zu diesem Adressbereich sind möglich, wenn Sie diesen im Listenfeld selektieren und auf den Schalter „Bearbeiten“ klicken. Soll ein bestehender Eintrag gelöscht werden , so ist es auch hier notwendig, erst in die Bearbeitungsmaske des Eintrages zu wechseln und über Schalter „Zone löschen“ diesen zu entfernen.



Wie auch bei den „verwalteten Domains“ können hier individuelle Einstellungen vorgenommen werden.

Zonentransfers erlauben von folgenden IP-Adressen aus

Sofern der DNS-Server des DEFENDO als „offizieller“ DNS-Server im Verbund des Internet-Domain-Name-Services fungiert, müssen die sekundären DNS-Server die DNS-Informationen des verwalteten IP-Adress-Bereiches herunterladen können. Geben Sie hier die IP-Adressen der DNS-Server ein, die berechtigt sind, einen Zonentransfer durchzuführen.

> *Hinweis:*
>
> *Zusätzlich ist im Firewall der TCP-Port 53 freizugeben um Zonentransfers zu ermöglichen.*

Benutzer Einträge

Um einen PTR-Record zu definieren, tragen Sie bitte die im IP-Adressbereich auf eine vollständige IP-Adresse fehlenden Zahlen in umgekehrter Reihenfolge ein (um z.B. im Bereich 172.16 die Adresse 172.16.5.10 zu definieren ist hier 10.5 einzugeben). Wählen Sie PTR aus und tragen Sie in das letzte Feld den zugehörigen Hostnamen mit

abschließendem Punkt ein. Um einen DNS-Server zu definieren, tragen Sie den zugehörigen Adressbereich als vollständige in-addr.arpa.-Adresse in das erste Feld ein (z.B. 5.16.172.in-addr.arpa. um einen Nameserver für den Bereich 172.16.5 zu definieren. Vergessen Sie nicht den abschließenden Punkt), wählen Sie NS aus und tragen Sie in das letzte Feld den DNS-Namen dieses Name-Servers ein.

Drücken Sie auf Hinzufügen um neue Einträge zu aktivieren. Wählen Sie einen Eintrag aus der Liste aus und drücken Sie auf Entfernen um den Eintrag zu löschen.

Start of Authority

Mit Hilfe dieses Wertes konfigurieren Sie den Hostnamen der im SOA-Record der Domain hinterlegt werden soll. Wählen Sie Grundeinstellung um den aktuellen Hostnamen zu verwenden oder wählen Sie den Optionsschalter vor dem Eingabefeld und geben Sie dort den Hostnamen für den SOA-Record ein.

Startwert Serial

Jede DNS-Zone verfügt über eine fortlaufende Versionsnummer, anhand derer sekundäre DNS-Server entscheiden, ob eine aktueller Version verfügbar und damit ein Zonentransfer notwendig ist. Diese Versionsnummer wird vom DEFENDO automatisch erhöht. Das Eingabefeld „Startwert Serial“ zeigt jeweils den aktuellen Wert an und ermöglicht es diesen zu Verändern.

Nameserver

Hier konfigurieren Sie die Nameserver für die aktuelle Domain. Ist einer der Nameserver der DEFENDO selbst, so kann dieser Wert aus den Grundeinstellungen bezogen werden. Wählen Sie den Optionsschalter vor dem Eingabefeld um einen anderen Wert zu vergeben. Weitere Nameserver-Einträge können in den folgenden Eingabefeldern eingetragen werden.

Fehlende PTR-Einträge automatisch ergänzen mit ...

Alle Adressen, die nicht mit Hilfe von PTR-Einträgen manuell auf Namen zugewiesen wurden, lassen sich mit Hilfe dieser Einstellung automatisch zuweisen. Tragen Sie zunächst den Basis-Hostname ein. Diesem wird der IP-Teil aus dem PTR-Record angefügt. Die Domain wird entweder aus den Grundeinstellungen übernommen oder kann manuell vergeben werden, wenn der Optionsschalter vor dem Eingabefeld gesetzt wird. Bitte beachten Sie, daß der Domain automatisch ein abschließender Punkt anfügt wird.

Öffentliche Zone

DNS-Anfragen an diese Zone sind normalerweise nur aus den lokalen IP-Netzwerken die in den Grundeinstellungen konfiguriert sind erlaubt. Sollen DNS-Anfragen von beliebigen IP-Adressen aus möglich sein, so ist die Zone als „öffentlich“ zu markieren.

> *Hinweis:*
>
> *Um DNS-Anfragen aus dem Internet an den DNS-Server des DEFENDO zu ermöglichen ist je nach Konfiguration. im Firewall zusätzlich der UDP-Port 53 freizugeben.*

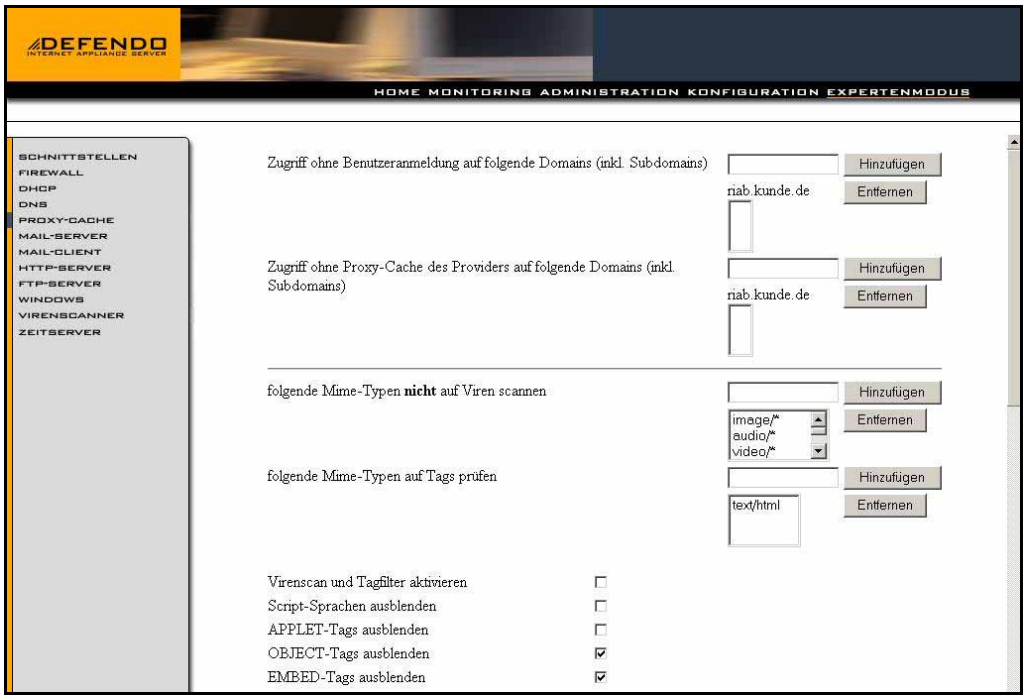
Drücken Sie auf OK um Änderungen zu aktivieren oder wählen Sie Zone löschen um die gesamte DNS-Zone mitsamt aller Einträge zu löschen.

12.5. Proxy-Cache

Der Proxy-Cache des DEFENDO ermöglicht es Ihnen den Zugriff von Rechnern im LAN auf das Internet genauer zu Reglementieren. Zusätzlich werden aufgerufene statische Webseiten auf dem DEFENDO für eine gewisse Zeit zwischengespeichert, so dass ein erneutes Aufrufen dieser Seiten keinen erneuten Zugriff auf das Internet erforderlich macht. Dadurch wird die Netzauslastung gesenkt und der Seitenzugriff für den Benutzer wesentlich beschleunigt. Durch das Proxy-Konzept wird ferner die direkte Verbindung zwischen dem Browser im LAN und dem Web-Server im Internet durch den DEFENDO unterbrochen, was die Sicherheit der Verbindung erhöht. Der Browser kommuniziert ausschließlich mit dem Proxy-Cache, der Proxy-Cache wiederum kommuniziert über eine separate Verbindung mit den Servern im Internet. Es werden folgende Protokolle unterstützt: http, https (Sicherheit), ftp (nur download), gopher und wais. Bitte beachten Sie, daß Ihr Browser zur Benutzung des Proxy-Caches entsprechend zu konfigurieren ist.

Ein Hinweis zur Zwischenspeicherung von Seiten im Proxy-Cache: Nicht gespeichert werden verschlüsselte Seiten, Seiten auf die nur mit Benutzeranmeldung zugegriffen werden darf, Seiten die eine bestimmte konfigurierbare Größe überschreiten und Seiten die auf Anweisung des zugehörigen Web-Server nicht gespeichert werden dürfen (häufig bei Zählern oder Werbebannern der Fall). Gespeicherte Seiten werden vom Web-Server neu bezogen, wenn der Browser eine entsprechende Abfrage abschickt (Aktualisieren). Befindet sich eine Seite bereits seit

mehreren Stunden im Cache, wird beim Web-Server angefragt, ob sich die Seite seit dem letzen Zugriff verändert hat. Seiten werden aus dem Cache gelöscht, wenn ein vom Server bestimmtes Verfallsdatum überschritten ist, eine Seite bereits seit mehreren Tage im Cache liegt oder kein Platz mehr im Cache ist und auf die Seite am längsten nicht mehr zugegriffen wurde. Bitte beachten Sie, daß Seiten häufig auch im Cache Ihres Browsers zwischengespeichert werden. Sollten Ihnen veraltete Seiten angezeigt werden, so hat sich wiederholt der Browser selbst als Ursache ergeben. Löschen Sie daher bitte zunächst den Cache Ihres Browsers.



Der oberste Teil der Maske ermöglicht Ihnen den Zugriff auf bestimmte Adressen zu reglementieren. Im Bereich „Zugriff ohne Benutzeranmeldung“ können Sie Hostnamen, Domains oder IP-Adressen eintragen für die keine Benutzeranmeldung notwendig ist. Hier ist kein Eintrag erforderlich, wenn die Proxy-Benutzeranmeldung ohnehin ausgeschaltet ist. Die eingabe von Hostnamen und Domains bezieht stets Subdomains mit ein. Wird also beispielsweise provider.de in die Liste eingetragen, so ist z.B. auch der Zugriff auf www.provider.de ohne Paßwort möglich. Sollten Sie den URL-Filter aktiviert haben, so beachten Sie bitte, daß Zugriffe ohne Benutzeranmeldung stets gegen die Proxylisten der Gruppe „system-proxy“ geprüft werden. Geben Sie einen Hostnamen oder eine Domain ein und drücken Sie auf Hinzufügen um die Liste zu erweitern. Der Hostname des DEFENDO selbst ist immer Bestandteil dieser Liste. Wählen Sie einen Eintrag aus der Liste und drücken Sie Entfernen um ihn zu löschen.

Der Bereich „Zugriff ohne Proxy-Cache des Providers“ kann dazu verwendet werden, auf bestimmte Adressen (z.B. aus dem Intranet) stets direkt zuzugreifen. Ein vorgeschalteter Proxy oder Firewall der als „Proxy-Cache des Providers“ weiter unten in dieser Bildschirmmaske konfiguriert ist, wird bei Zugriffen auf hier angegebene Domains nicht angesprochen. Hier ist kein Eintrag erforderlich, wenn ohnehin kein vorgeschalteter „Proxy-Cache des Providers“ verwendet wird. Der Eintrag bezieht sich stets auch auf Subdomains. Wird also beispielsweise provider.de in die Liste eingetragen, so erfolgt z.B. auch der Zugriff auf www.provider.de unter Umgehung des übergeordneten Proxy-Caches. Der Hostname des DEFENDO selbst ist immer Bestandteil dieser Liste. Geben Sie einen Hostnamen oder eine Domain ein und drücken Sie auf Hinzufügen um die Liste zu erweitern. Wählen Sie einen Eintrag aus und drücken Sie Entfernen um ihn zu löschen.

Der folgende Bereich bezieht sich auf die Konfiguration des Virenscanners und Tag-Filters des DEFENDO Proxy-Caches. Hinterlegen Sie ein Liste von Mime-Typen, die nicht auf Viren geprüft werden sollen. Die Angabe erfolgt im Format Haupttyp/Untertyp, wobei als Haup- oder Untertyp auch ein Stern (*) für einen beliebigen Typen angegeben werden kann (z.B. image/* für beliebige Bildformate). Wird bei einer angeforderten Web-Seite ein Mime-Type übermittelt, der sich nicht in dieser Liste befindet, so wird diese Datei auf Viren überprüft sofern der Virenscanner auf dem DEFENDO installiert ist und der Proxy-Virenscan aktiviert ist. Um einen weiteren Mime-Typen vom Virenscan auszuschließen, tragen Sie diesen in das Eingabefeld ein und drücken Sie auf Hinzufügen. Soll nur der Tagfilter benutzt und der Virenscan komplett deaktiviert werden, fügen Sie bitte den Mime-Typ */* hinzu. Um einen Mime-Typ aus der Liste zu löschen, markieren Sie diesen und drücken Sie auf Entfernen.

Achtung:

Benutzer des Microsoft Internet-Explorer ab Version 5 können mit rechter Maustaste über einem FTP-Link die Funktion „Kopieren nach Ordner...“ ausführen. Diese Funktion aktiviert einen direkten FTP-Download unter Umgehung des Proxy-Caches. Sollte im Firewall der direkte FTP-Zugriff freigegeben sein werden auf diese Weise angeforderte Downloads nicht auf Viren gescannt! Ist der direkte FTP-Zugriff im Firewall nicht erlaubt, so scheitert der Download über diese Funktion.

Um potentiell gefährliche Tags aus HTML-Seiten zu entfernen, kann in der folgenden Liste angegeben werden, in welchen Dateiarten nach

Tags gesucht werden soll. Geben Sie analog zur vorhergehenden Liste die gewünschten Mime-Typen an bzw. enfernen Sie diese. Wird eine Datei mit dem hier angegebenen Mime-Typ empfangen, so werden die konfigurierten Tags ausgeblendet sofern der Tag-Filter aktiviert wurde.

Setzen Sie einen Haken bei „Script-Sprachen ausblenden“, wenn Sie den HTML-Tag <SCRIPT> sowie alle Event-Handler in weiteren Tags unkenntlich machen wollen. Ein Haken bei APPLET-, OBJECT- bzw. EMBED-Tags ausblenden macht die gleichnamigen Tags unkenntlich.

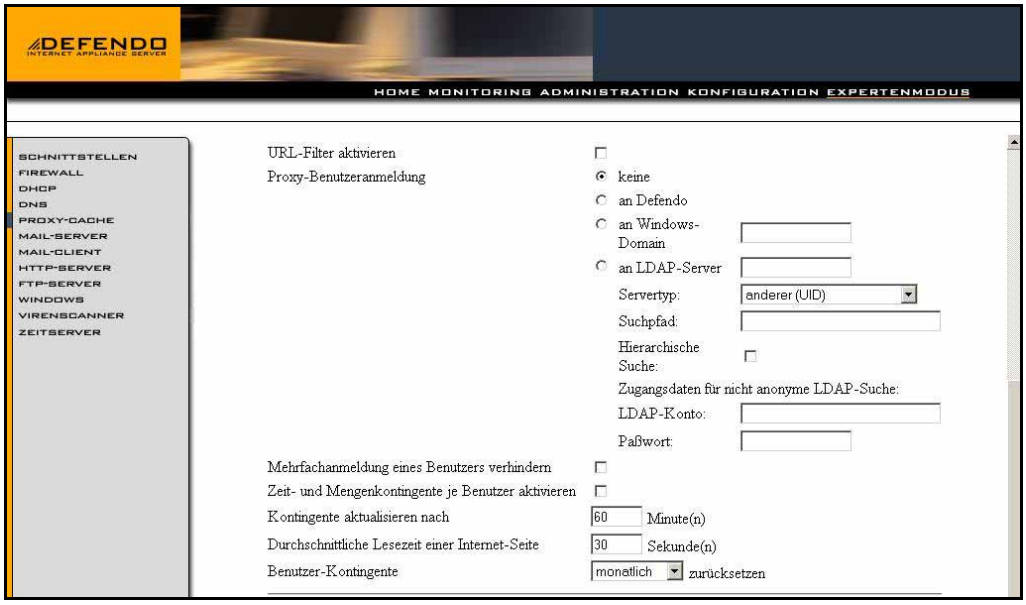
Um sowohl den Proxy-Virenscan als auch den Tag-Filter zu aktivieren, setzen Sie einen Haken bei der entsprechenden Option. Bitte beachten Sie, daß durch Aktivierung des Tag-Filters die Funktionalität von manchen Web-Seiten die auf ausgeblendete Tags beruht gestört werden kann.

Hinweis:

Diese Funktion kann erst genutzt werden, wenn ein Virenscanner auf dem DEFENDO installiert ist. Die Lizenzen für den Virenscanner sind nicht im DEFENDO enthalten und müssen separat erworben werden. Siehe hierzu auch Kapitel 12.11.

Bei aktiviertem Proxy-Virenscan bzw. Tag-Filter ist die Option „Mehrfachanmeldung eines Benutzers verhindern“ außer Funktion.

Über den Schalter „URL-Filter aktivieren“ lassen sich die Proxylisten aktivieren, die über die Gruppenverwaltung Benutzerkreisen zugeordnet werden. Bitte beachten Sie hierzu die Hinweise im folgenden Absatz zur Benutzeranmeldung.



Mit Hilfe der Optionen unter „Proxy-Benutzeranmeldung“ ist es möglich, den Zugriff via Proxy auf das Internet mit Benutzername und Kennwort zu belegen. Es stehen verschiedene Optionen zur Verfügung:

Keine Benutzeranmeldung

Der Zugriff auf das Internet ist von allen lokalen IP-Adressen via Proxy ohne Anmeldung möglich. Es ist in diesem Falle nicht notwendig, Benutzerkonten für den Proxy-Zugriff (Gruppe system-proxy) anzulegen. Sollten Sie den URL-Filter (Proxylisten) zur Einschränkung des Zugriffs verwenden, so ist dieser nicht gruppenbasierend einsetzbar, da ja keine Benutzerauthentifizierung stattfindet. Um den Internet-Zugriff mit Hilfe der Proxylisten dennoch zu bschränken, sind die gewünschten Listen der Gruppe system-proxy zuzuordnen. Die Einschränkungen gelten damit für alle Benutzer.

Benutzeranmeldung an DEFENDO

Bei Auswahl dieser Option ist der Zugriff in das Internet von allen lokalen IP-Adressen möglich, wenn sich der Benutzer mit Kennwort authentifiziert hat. Die Konten und Paßwörter sind dazu in der DEFENDO Benutzerverwaltung einzurichten (Gruppe system-proxy).

Benutzeranmeldung an Windows-Domain

Ist diese Option gewählt, so ist der Zugriff auf das Internet von allen lokalen IP-Adresse aus möglich, wenn der Benutzer mit seinem Windows-Benutzernamen und seinem Windows-Kennwort Zugriff auf eine bestimmte Datei hat. Tragen Sie dazu bitte in das entsprechende Feld der DEFENDO-Konfigurationsoberfäche Ihre Windows-Domain ein. Erstellen Sie ferner auf der NETLOGON-Freigabe Ihres Windows-

Domain-Controllers eine Datei mit Namen proxyauth. Diese Datei muß ausschließlich das Wort allow enthalten. Vergeben Sie nun Leseberechtigung auf diese Datei für all die Benutzer, die Zugriff auf das Internet erhalten sollen. Das Anlegen von Konten auf dem DEFENDO in der Gruppe system-proxy ist für die reine Anmeldung nicht erforderlich. Sollten Sie jedoch den URL-Filter mit seinen Proxylisten verwenden, so kann es notwendig werden, manche oder alle Benutzer auch auf dem DEFENDO anzulegen. Für alle Benutzer gelten nämlich die Proxylisten, die der Gruppe system-proxy zugeordnet wurden. Sollen für einzelne Benutzer weitere Listen gelten, so sind entsprechende Benutzer auf dem DEFENDO anzulegen und der Gruppe system-proxy zuzuordnen. Das Paßwort mit dem die Konten auf dem DEFENDO angelegt werden spielt in diesem Falle keine Rolle.

Benutzeranmeldung an LDAP-Server

Ist diese Option gewählt, so ist der Zugriff auf das Internet von allen lokalen IP-Adresse aus möglich, wenn der Benutzer sich gegenüber einem LDAP-Server authentifizieren kann. Tragen Sie dazu bitte in das entsprechende Feld der DEFENDO-Konfigurationsoberfäche die IP-Adresse oder den DNS-Namen Ihres LDAP-Servers ein. Wählen Sie nun den Typ des LDAP-Servers. Der Typ „anderer“ authentifiziert den Benutzer gegen Objekte anhand des Attributs „UID“. Wählen Sie den Typ „MS ActiveDirectory (CN)“ oder „MS ActiveDirectory (SAM)“ wenn das Benutzer-Objekt anhand des Attributs „CN“ identifiziert wird. Im Microsoft ActiveDirectory entspricht das Attribut „CN“ dem nachträglich nicht mehr änderbaren Namen für das Benutzerobjekt. Die Verwendung dieses Attributes als Benutzerkennung kann problematisch werden, da hier Sonderzeichen und Leerzeichen enthalten sein können. Bei der Auswahl von „MS ActiveDirectory (SAM)“ wird das Benutzerobjekt daher anhand des Attributs „sAMAccountName“ im ActiveDirectory gesucht. In der Benutzerverwaltung wird dieses Attribut als „Benutzeranmeldename Windows NT 3.5x/4.0“ geführt. Bitte beachten Sie, daß die Suchfunktion an bestimmte Berechtigungen im LDAP-Server geknüpft ist. Ist der lesende Zugriff auf ein Benutzerobjekt nicht möglich, so ist eine Anmeldung als dieser Benutzer nicht möglich.

Für die Verwendung der LDAP-Authentifizierung ist ferner die Angabe des Suchpfades erforderlich. Geben Sie hier den für Ihren LDAP-Server benötigten Pfad ein. Beispiele hierzu:

cn=users,dc=Ihre,dc=LDAP,dc=Domain

ou=people,dc=Ihre,dc=LDAP,dc=Domain

In dem hier angegebenen Container müssen die Benutzerobjekte abgelegt sein. Sollten die Benutzerobjekte dort hierarchisch abgelegt sein, so aktivieren Sie bitte die Option „Hierarchische Suche“.

Die hierarchische Suche bzw. die Suche des Benutzerobjekts anhand des Attributs „sAMAccountName“ erfordert die Berechtigung, den Suchpfad anonym durchsuchen zu dürfen (im ActiveDirectory bedeutet dies Leseberechtigung für „Jeder“). Ist dies nicht gegeben oder gewünscht, so muß sich der LDAP-Client am LDAP-Server anmelden. Geben Sie dazu in die entsprechenden Felder das LDAP-Konto mit dem zugehörigen Paßwort ein. Bitte beachten Sie, daß Sie als LDAP-Konto den kompletten distinguished Name (DN) des Kontos eingeben müssen und dieser keine Leerzeichen enthalten darf. Beispielsweise:

cn=proxy,cn=users,dc=Ihre,dc=LDAP,dc=Domain

Die Benutzerobjekte müssen entsprechend mit Lesezugriff für dieses Konto ausgestattet werden. Benutzerobjekte die mangels Lesezugriff bei der Suche nicht gefunden werden, werden auch bei der Anmeldung nicht berücksichtigt.

Das Anlegen von Konten auf dem DEFENDO in der Gruppe system-proxy ist für die reine Anmeldung nicht erforderlich. Sollten Sie jedoch den URL-Filter mit seinen Proxylisten verwenden, so kann es notwendig werden, manche oder alle Benutzer auch auf dem DEFENDO anzulegen. Für alle Benutzer gelten nämlich die Proxylisten, die der Gruppe system-proxy zugeordnet wurden. Sollen für einzelne Benutzer weitere Listen gelten, so sind entsprechende Benutzer auf dem DEFENDO anzulegen und der Gruppe system-proxy zuzuordnen. Das Paßwort mit dem die Konten auf dem DEFENDO angelegt werden spielt in diesem Falle keine Rolle.

Der Schalter „Mehrfachanmeldung eines Benutzers verhindern“ bindet ein Benutzeranmeldung für 10 Minuten an die IP-Adresse von der aus der letzte Zugriff stattgefunden hat. Erfolgt innerhalb dieser Zeitspanne ein Zugriff von einer anderen IP-Adresse aus, besteht die Möglichkeit, daß der Benutzer seine Anmeldedaten weitergegeben hat. Der Zugriff wird daher gesperrt.

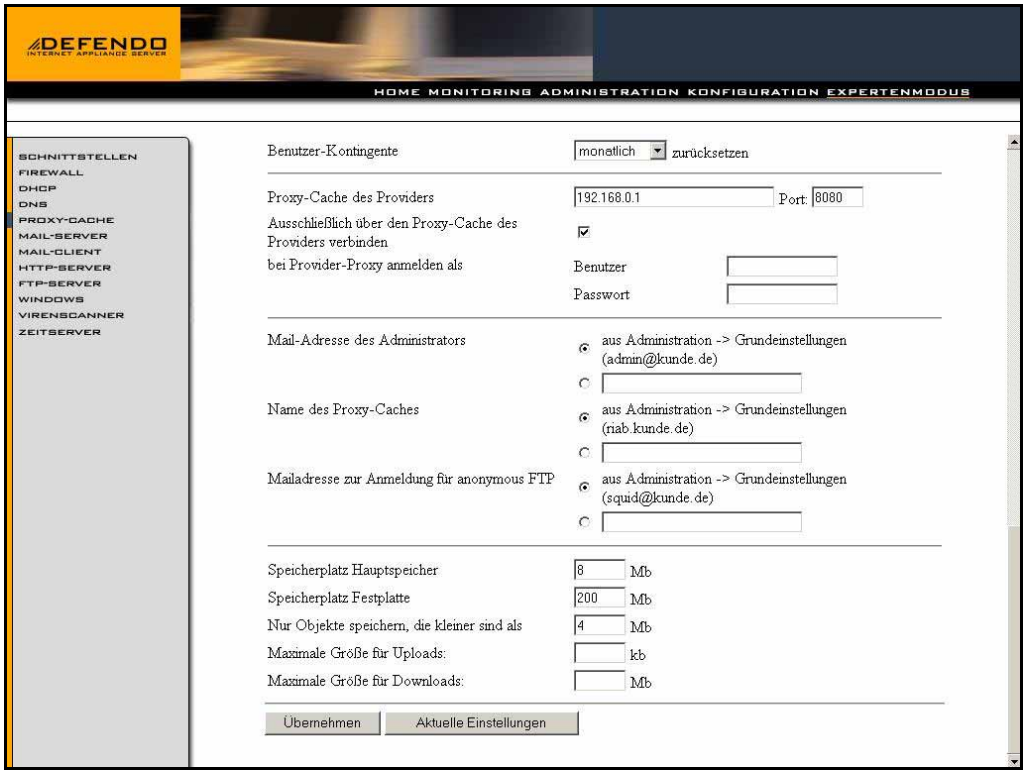
> *Hinweis:*
>
> *Ist die Option „Virenscan und Tagfilter aktivieren“ gewählt, läßt sich die Mehrfachanmeldung eines Benutzers nicht verhindern.*

Bei aktivierter Benutzeranmeldung an DEFENDO können ferner die „Zeit- und Mengenkontingente je Benutzer“ zugeschaltet werden. Die

Kontingente werden ebenfalls in der Benutzerverwaltung festgelegt. Um Ressourcen zu schonen, können Sie ferner angeben, in welchem Abstand die aktuell verbrauchten Kontingente je Benutzer aktualisiert werden sollen. Geben Sie den gewünschten zeitlichen Abstand bei „Kontingente aktualisieren nach“ ein. Zur Bestimmung des verbrauchten Zeitkontingents eines Benutzers wird zum einen die reine Ladezeit der angeforderten Dateien verwendet. Tragen Sie bei „durchschnittliche Lesezeit einer Internet-Seite“ den Wert ein, der maximal auf die Ladezeit einer Seite aufgeschlagen werden soll. Wird innerhalb der hier angegebenen Zeitspanne erneut ein Zugriff vom gleichen Benutzer registriert, so wird lediglich die Zeitspanne bis zu diesem Zugriff aufgeschlagen. Wenn Sie hier den Wert 0 eintragen, wird dem Benutzer ausschließlich die reine Ladezeit auf sein Kontingent angerechnet. Wählen Sie mit Hilfe der folgenden Auswahlliste aus, wann die Benutzerkontingente automatisch zurückgesetzt werden sollen.

Hinweis:

Ist die Benutzeranmeldung deaktiviert, so bleiben die Zeit- und Mengenkontingente wirkungslos. Auch bei Benutzeranmeldung an Windows-Domäne oder LDAP kann diese Funktion nicht genutzt werden.



Bietet Ihnen Ihr Provider seinen Proxy-Cache zur Verwendung an, so können Sie zur Erhöhung des Durchsatzes den Proxy-Cache des

DEFENDO so konfigurieren, daß er sich über den „Proxy-Cache des Providers“ in das Internet verbindet. Geben Sie dessen Namen oder IP-Adresse und den Port in den entsprechenden Feldern ein. Da wie bereits erwähnt bestimmte Seiten nicht in einem Cache abgelegt werden dürfen, werden diese Seiten dabei nach wie vor direkt vom Web-Server im Internet abgeholt. Ist dies nicht erwünscht, weil z.B. eine entsprechend reglementierte vorgelagerte Firewall den direkten Zugriff auf Web-Server für den DEFENDO unmöglich macht, so setzen Sie bitte einen Haken bei „Ausschließlich über den Proxy-Cache des Providers verbinden“. Falls erforderlich kann sich der Proxy-Cache des DEFENDO auch beim Proxy-Cache des Providers authentifizieren. Geben Sie den zugehörigen Benutzernamen und das Kennwort in die entsprechenden Felder ein. Ist keine Anmeldung am Proxy-Cache des Providers notwendig, so bleiben diese Felder leer.

Der Hostname und die Mail-Adresse des Administrators die der Proxy-Cache bei Fehlermeldungen präsentieren können aus den Grundeinstellungen bezogen werden. Alternativ setzen Sie den Optionsschalter vor dem Eingabefeld und geben Sie selbst einen Namen an.

Beim Zugriff auf FTP-Server mit anonymem Zugriff wird von den FTP-Servern die Angabe einer Mail-Adresse als Paßwort gefordert. Sie können diese aus den Grundeinstellungen beziehen oder selbst eine Adresse in das Eingabefeld eintragen. Setzen Sie den Optionsschalter vor der gewünschten Einstellung.

Geben Sie über die entsprechenden Einstellungen an, wieviel Speicherplatz der Proxy-Cache im Hauptspeicher und auf der Festplatte belegen darf. Physikalisch werden die Seiten im Verzeichnis /var/spool/squid/ auf der Festplatte abgelegt. Überprüfen Sie bitte den freien Speicherplatz in der entsprechenden Festplattenpartition für diesen Bereich unter Monitoring -> Systeminfo (siehe Kapitel 10.3) bevor Sie diesen Wert erhöhen.

Um eine schnelle Überfüllung des Caches zu vermeiden, werden Dateien die eine bestimmte Größe überschreiten nicht zwischengespeichert. Geben Sie diese Größe bei „Nur Objekte speichern die kleiner sind als“ an.

Die „maximale Größe für Uploads“ beschränkt die Größe von POST- und PUT-Request mit deren Hilfe Dateien oder Formularparameter übermittelt werden.

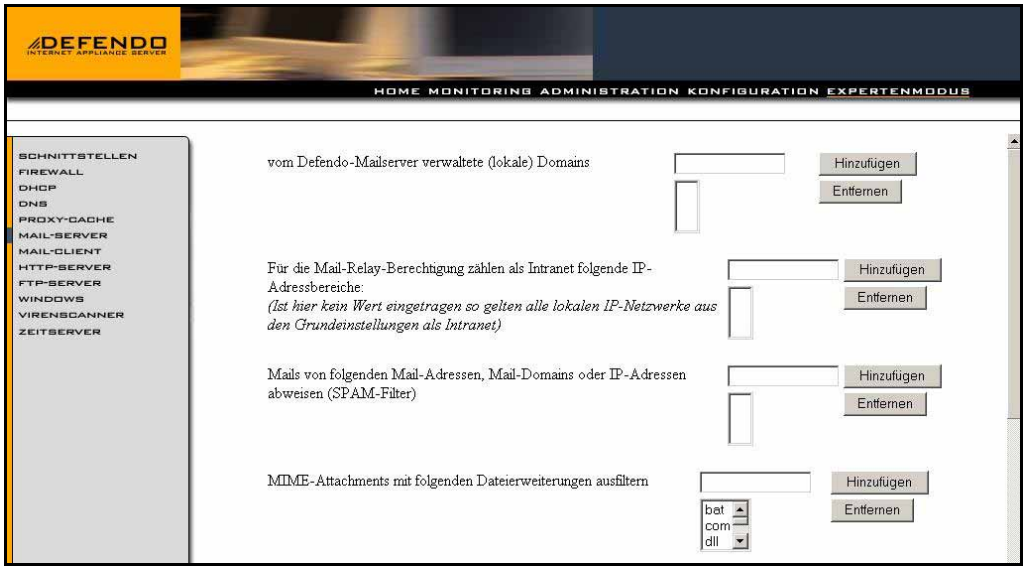
Die „maximale Größe für Downloads“ beschränkt die Größe von Dateien die von einem Server aus dem Internet heruntergeladen werden. Im allgemeinen teilt der Server im Internet die Größe der übermittelten Daten bereits im Voraus mit, so daß eine Fehlermeldung beim Überschrei-

ten der zulässigen Größe generiert werden kann. Ist die Größe der angeforderten Daten jedoch im Vorfeld nicht bekannt, so wird der laufende Download beim Erreichen der Schranke kommentarlos abgebrochen.

Drücken Sie auf „Übernehmen“ um Änderungen zu aktivieren oder „Aktuelle Einstellungen“ um die derzeit verwendeten Einstellungen anzuzeigen.

12.6. Mail-Server

Der SMTP-Mail-Server des DEFENDO wird über diesen Menüpunkt konfiguriert.



Im oberen Maskenbereich konfigurieren Sie die „vom DEFENDO-Mailserver verwalteten (lokalen) Domains“. Mails an diese Domains werden nicht weitergesendet sondern an ein lokales POP3/IMAP4-Konto bzw. einen lokalen Mail-Verteiler des DEFENDO zugestellt. Dient der DEFENDO Mails lediglich als Mail-Gateway, das eingehende Mails an einen internen Mail-Server in Ihrem LAN weiterleitet, so dürfen die für den internen Mail-Server bestimmten Domains hier nicht eingetragen werden. Um eine neue lokale Domain hinzuzufügen, tragen Sie diese bitte in das entsprechende Eingabefeld ein und drücken Sie auf „Hinzufügen“. Wählen Sie eine Domain aus und drücken Sie auf „Entfernen“, um Mails an diese Domain nicht mehr lokal zuzustellen.

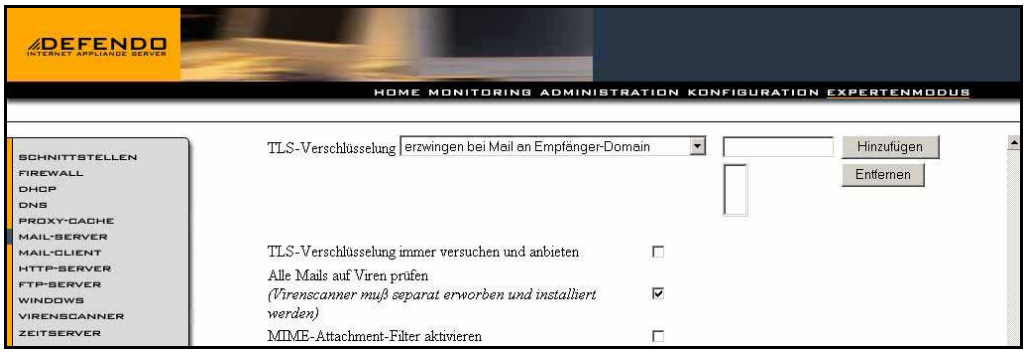
Normalerweise werden vom Mail-Server alle IP-Adressen die in den Grundeinstellungen als lokale IP-Adressen konfiguiert wurden als Intranet betrachtet. Nur von diesen internen Adressen aus dürfen eMails in

das Internet versendet werden. Allen anderen Adressen ist es nicht erlaubt, eMail in das Internet zu versenden. Auf diese Weise wird verhindert, dass der Mail-Server als Relay-Server für den Versand von SPAM-Mails missbraucht wird. Sollen von den Grundeinstellungen abweichende IP-Adressbereiche das Relay-Recht erhalten, so lassen sich diese hinterlegen. Mit Hilfe dieser Einstellung ist es auch möglich, nur bestimmten Computern im LAN den Mail-Versand in das Internet zu erlauben, während alle anderen Computer nur interne Mails versenden dürfen. Tragen Sie im entsprechenden Feld der Maske IP-Netzwerke mit Netzmaske (z.B. 192.168.0.128/255.255.255.128), IP-Adressbereiche (z.B. 192.168.1.3-192.168.1.11) oder einzelne IP-Adressen ein. Drücken Sie dann auf „Hinzufügen“ um diesen Eintrag zu aktivieren. Nur die eingetragenen IP-Adressen werden dann von der Relay-Kontrolle als Intranet betrachtet. Wählen Sie einen Eintrag aus und drücken Sie auf „Entfernen“ um die betroffenen Adressen aus dem Intranet-Bereich zu entfernen. Wenn kein Eintrag mehr vorhanden ist, werden wieder alle lokalen Netwerke aus den Grundeinstellungen als Intranet betrachtet.

Die Annahme von bestimmten Mails läßt sich mit Hilfe des SPAM-Filters verhindern. Geben Sie einzelne Mail-Adressen (z.B. spammer@spam.com) ein um Mails von diesem Absender abzulehnen. Die Angabe einer kompletten Domain (z.B. spam.com) stoppt alle Mails mit einer Absenderadresse aus dieser Domain oder Subdomains (also z.B. spammer@spam.com oder info@www.spam.com). Ferner lassen sich auch IP-Adressen eingeben, um Mails abzuweisen die von der entsprechenden Adresse aus geschickt wurden. Geben Sie den gewünschten Wert an und drücken Sie auf den Schaltern „Hinzufügen“ um die entsprechenden Mails zu blockieren. Wählen Sie einen Eintrag aus der Liste und drücken Sie auf den zugehörigen Schalter „Entfernen“ um den Eintrag wieder freizugeben.

Dateianhänge im MIME-Format können basierend auf Ihrem Dateinamen ausgefiltert werden. Im Bereich „MIME-Attachments mit folgenden Dateierweiterungen ausfiltern“ kann angegeben werden, welche Dateien den Mail-Server nicht passieren dürfen. Um eine neue Dateierweiterung zu Filtern geben Sie diese bitte im Format ext, .ext oder *.ext an und drücken Sie „Hinzufügen“. Wählen Sie eine Dateierweiterung aus und drücken Sie „Entfernen“ um diese wieder zuzulassen. Erreicht eine Mail mit zu filterndem Dateianhang den Mail-Server, so wird der Dateianhang durch eine Textmeldung ersetzt, die auf die Veränderung hinweist. Die Mail wird dann in dieser veränderten Form an den Empfänger zugestellt. Der entfernte Dateianhang kann vom Benutzer admin per FTP, telnet oder über die Konsole im Verzeichnis quarantine eingesehen werden. Dieses Verzeichnis wird automatisch nach 10 Tagen bereinigt.

Der Versand von Mails erfolgt im Normalfall über das Mail-Relay Ihres Providers bzw. mit Hilfe der Mailexchanger-Informationen aus dem DNS. Um die Mail-Weiterleitung für bestimmte Domains selbst zu bestimmen, kann ein Mail-Routing eingetragen werden. Tragen Sie zunächst die gewünschte Mail-Domain ein (der Teil einer Mail-Adresse nach dem @). Wählen Sie dann aus der Liste aus, wie mit Mails an diese Domain verfahren werden soll. Ist „mit SMTP an Mail-Server“ ausgewählt, so können Sie in das darauf folgende Eingabefeld den DNS-Namen oder die IP-Adresse des Mail-Servers eintragen, an den Mails mit der angegebenen Domain geschickt werden sollen. Die Einstellung „mit SMTP sofort versenden an Mail-Server“ ist identisch, jedoch werden Mails an die hier bestimmte Domain immer sofort versendet, auch wenn ausgehende Mails normalerweise gesammelt werden. Wählen Sie diese Einstellung, wenn der DEFENDO als Mail-Relay für einen internen Mail-Server in Ihrem LAN dient. Drücken Sie auf „Hinzufügen“ um ein neues Mail-Routing zu aktivieren oder wählen Sie ein Routing aus der Liste aus und drücken Sie auf „Entfernen“ um ein Mail-Routing zu löschen.



Der DEFENDO unterstützt die verschlüsselte Übermittlung von Mail mit Hilfe des STARTTLS-Befehls. Dabei wird jedoch nur die Verbindung mit dem unmittelbaren Kommunikationspartner des SMTP-Mail-Server des DEFENDO verschlüsselt. Es handelt sich dabei also weder um eine durchgängige Verschlüsselung vom Absender bis zum Empfänger der Mail, noch ermöglicht es diese Option die Authentizität der Mail festzustellen.

Die Verschlüsselung ausgehender Mails kann für Mails an eine bestimmte Empfängerdomain erzwungen werden. Wählen Sie dazu im Bereich TLS-Verschlüsselung die entsprechende Option und geben Sie die Mail-Domain (der Teil einer Mail-Adresse nach dem @) ein. Drücken Sie dann auf „Hinzufügen“. Diese Einstellung empfiehlt sich, wenn der Mail-Versand zu der Empfänger-Domain nicht unbedingt an einen bestimmten Ziel-Server gebunden ist (z.B. weil ein Backup-Mail-Server existiert). Unterstützt der angesprochene Mail-Server keinen verschlüsselten Mail-Versand, wird die Mail zurückgehalten und zu einem späte-

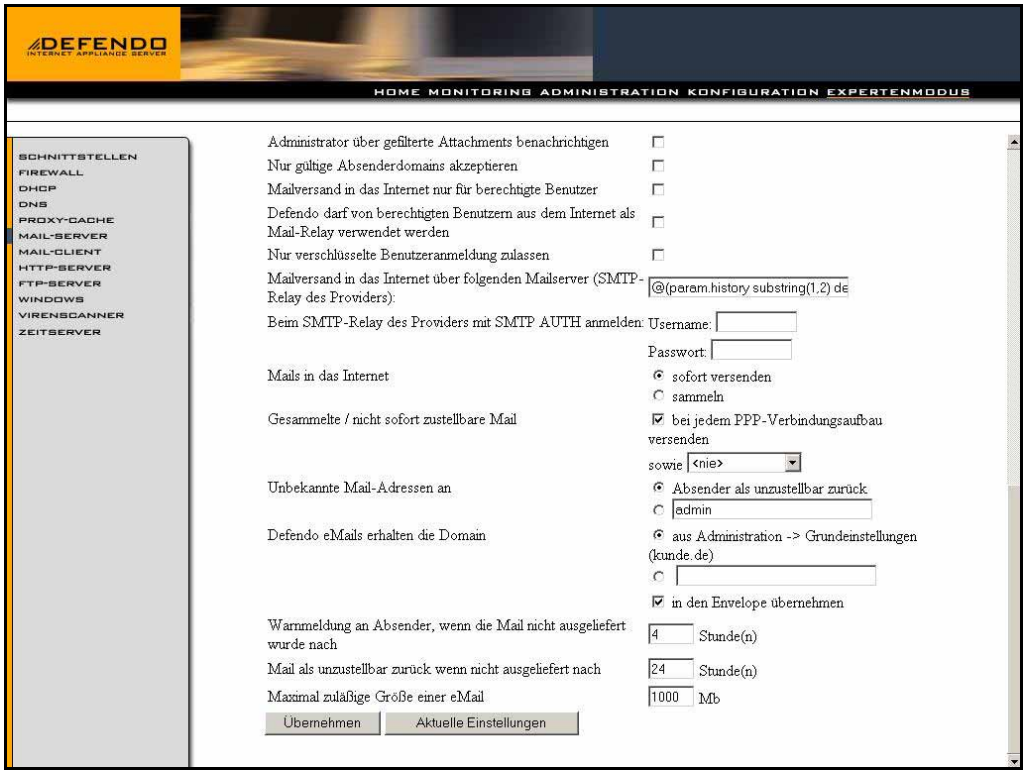
ren Zeitpunkt nocheinmal versucht zuzustellen. Möglich ist es ferner, die verschlüsselte Kommunikation mit einem bestimmten Mail-Server bzw. –Client zu erzwingen. Geben Sie hier einen Servernamen (nicht die Mail-Domain) oder eine IP-Adresse ein. Anders als bei der vorherigen Option wird die verschlüsselte Kommunikation hier auch bei eingehenden Mails erzwungen. Schließlich kann die verschlüsselte Kommunikation mit bestimmten Server unterbunden werden. Auch hier kann ein Servername oder eine IP-Adresse angegeben werden. Die verschlüsselte Nachrichtenübermittlung wird diesen weder angeboten noch von diesen akzeptiert.

Bei aktivierter Schaltfläche „TLS-Verschlüsselung immer versuchen und anbieten“ versucht der DEFENDO von sich aus ausgehende Mails verschlüsselt zu versenden wenn die Gegenstelle dies unterstützt und bietet diese Option bei allen eingehenden Mails grundsätzlich an. In diesem Falle entscheidet die Gegenstelle ob sie von dieser Option gebrauch macht.

Alle ein- und ausgehenden Mails (mit Ausnahme bestimmter vom System selbst generierten Mails) können auf Viren geprüft werden. Aktivieren Sie dazu bitte den entsprechenden Schalter. Die Virensuche erstreckt sich auch auf den Inhalt der gängigsten Archivformate wie ZIP oder GnuZip. Wird ein Virus gefunden, so wird die Mail temporär im Quarantäneverzeichnis virusmails gespeichert, das nur vom Benutzer admin über die Konsole, telnet oder FTP eingesehen werden kann. Sowohl der lokale admin als auch der Absender der Mail erhalten per Mail eine entsprechende Benachrichtigung über den Virusfund.

> *Hinweis:*
>
> *Diese Funktion kann erst genutzt werden, wenn ein Virenscanner auf dem DEFENDO installiert ist. Die Lizenzen für den Virenscanner sind nicht im DEFENDO enthalten und müssen separat erworben werden. Siehe hierzu auch Kapitel 12.11.*

Der Schalter MIME-Attachment-Filter aktivieren sorgt für Filterung der weiter oben konfigurierten Mail-Dateianhänge. Bitte beachten Sie, dass gesperrte Dateianhänge sowohl bei ein- als auch bei ausgehenden Mails gefiltert werden. Ist neben dem Attachment-Filter auch der Virenscanner aktiv, so werden Dateianhänge zunächst vom Virenscanner untersucht. Findet dieser einen Virus so wird die Mail wie üblich verworfen und sowohl der Absender als auch der admin per Mail darüber in Kenntnis gesetzt. Der Attachment-Filter erhält die virenverseuchte Mail erst gar nicht.



Auf Wunsch kann der admin per Mail über jeden gefilterten Dateianhang informiert werden. Aktivieren Sie dazu den entsprechenden Schalter.

Der Schalter „nur gültige Absenderdomains akzeptieren“ aktiviert eine Überprüfung des Domain-Teils der Absender-Mail-Adresse bei jeder eingehenden Mail. Existiert im DNS kein Eintrag für die Domain, so wird die Mail nicht angenommen. In Einzelfällen bietet diese Option Schutz vor unerwünschter Spam-Mail.

Achtung:

Es wird nicht die komplette Mail-Adresse sondern lediglich der Domain-Teil überprüft. Es kann so weder die Echtheit des Absenders gesichert werden, noch ist sichergestellt, dass Antworten an diese Adresse möglich sind.

Bitte beachten Sie, dass mit der Aktivierung dieser Option möglicherweise auch Mails abgewiesen werden, die Aufgrund von Unachtsamkeit eine falsche Absender-Domain tragen. Häufig tritt dieses Problem bei automatisch generierten Mails auf.

Es ist möglich, den Mail-Versand vom Intranet in das Internet nur bestimmten Benutzern zu erlauben, während nach wie vor jeder Benutzer lokal Mails verschicken darf. Aktivieren Sie dazu den Schalter „Mailversand in das Internet nur für berechtigte Benutzer“. Für den Versand von Mails aus den internen Netzen in das Internet ist dann eine SMTP AUTH Benutzeranmeldung notwendig. Wird keine Authentifizierungsinformation übermittelt, verweigert der Mail-Server den Versand der Mail in das Internet. Bitte beachten Sie, dass nicht jede Mail-Software die Benutzeranmeldung mit SMTP-AUTH unterstützt. Zur Festlegung, welche IP-Adressen vom Mail-Server als Intranet und welche als Internet betrachtet werden sollen, beachten Sie bitte den Konfigurationsbereich weiter oben in der Maske. Welche Benutzer bei Benutzeranmeldung als Berechtigt gelten, Mails durch den DEFENDO hindurchzuleiten, wird in der Benutzerverwaltung festgelegt (vgl. Kapitel 9.2.2.1).

Die Option „DEFENDO darf von berechtigten Benutzern aus dem Internet als Mail-Relay verwendet werden“ entspricht dem vorhergehenden Schalter. Hier wird jedoch geregelt, inwieweit bestimmte Benutzer von IP-Adressen die nicht zum Intranet zählen eMails über den DEFENDO in das Internet versenden dürfen. Diese Option ist z.B. für Außendienstmitarbeiter und Heimarbeitsplätze interessant. Ist diese Option nicht aktiviert, so wird der Mail-Versand von externen IP-Adressen aus in das Internet verweigert.

Wird „nur verschlüsselte Benutzeranmeldung zugelassen“, so wird die Benutzeranmeldung mit SMTP AUTH nur dann akzeptiert, wenn diese über TLS-Verschlüsselung vor dem Ausspähen gesichert ist. Andernfalls ist die Übertragung der Anmeldeinformationen im Klartext erlaubt.

Insbesondere bei der Internet-Anbindung über Wählleitung empfiehlt es sich, ausgehende Mails in das Internet über den Mail-Relay-Server Ihres Providers zu versenden. Geben Sie dessen Namen oder IP-Adresse bei „Mailversand in das Internet über folgenden Mailserver (SMTP-Relay des Providers)“ ein. Wenn Sie das Eingabefeld hingegen leer lassen, werden ausgehende Mails direkt an den laut DNS für die Empfängerdomain zuständigen Mail-Server zugestellt.

Sollte für die Nutzung des Relay-Server Ihres Providers eine Benutzeranmeldung mit SMTP AUTH erforderlich sein, so können Sie die den Benutzernamen und das Passwort in die entsprechenden Felder eintragen. Sind diese Felder leer, wird auch keine Benutzeranmeldung vorgenommen. In der Regel verlangt der Relay-Server eines Providers nur dann nach einer Benutzeranmeldung, wenn der Internetzugang über einen anderen Provider erfolgt. Es empfiehlt sich in diesem Falle, den Relay-Server des Providers einzutragen, über den der Internet-Zugang erfolgt.

Hinweis:

Die Benutzeranmeldung am Relay-Server Ihres Providers bezieht sich auf ausgehende Mails und hat nichts mit der Benutzeranmeldung zu tun, die Sie für die Abholung von Mails vom POP3-Server Ihres Providers benötigen. Sollten Sie wirklich eine Benutzeranmeldung für ausgehende Mails benötigen, so können diese Zugangsdaten aber durchaus mit denen des POP3-Servers identisch sein.

Ausgehende Mails können sofort in das Internet weitergeleitet oder gesammelt und zu einem späteren Zeitpunkt gebündelt versendet werden. Letzteres ist insbesondere bei der Anbindung an das Internet über eine Wählleitung interessant. Wählen Sie bitte den passenden Optionshaken.

Wann gesammelte Mails und Mails die zwar sofort gesendet werden sollten, jedoch aufgrund eines Übertragungsproblems nicht sofort gesendet werden konnten übertragen werden sollen, ist über die folgenden Optionen einstellbar. Wenn Sie über eine PPP-Wählverbindung mit dem Internet verbunden sind, kann dies bei jedem Verbindungsaufbau in das Internet geschehen. Aktivieren Sie dazu den entsprechenden Haken. Ferner kann der Mail-Versand in regelmäßigen Zeitabständen erfolgen. Wählen Sie eine Zeitspanne aus der Liste aus oder verwenden Sie den Wert <nie> um den Versand in bestimmten zeitlichen Abständen zu deaktivieren. Bei PPP-Wählverbindungen sollte mindestens eine der beiden Möglichkeiten zum Mail-Versand aktiv sein. Sie erkennen PPP-Wählverbindungen daran, daß als Default-Route eine Schnittstelle die mit ippp oder adsl beginnt eingetragen ist (siehe Kapitel 12.1). Sollten Sie nicht mit einer PPP-Wählverbindung an das Internet angeschlossen sein, so muß der Versand in bestimmten zeitlichen Abständen konfiguriert werden. Der Versand bei PPP-Verbindungsaufbau ist in diesem Falle wirkungslos.

Soll eine Mail an eine lokale Domain zugestellt werden und der Adressat existiert auf dem DEFENDO weder als Konto noch als Verteiler, so können Sie die Mail an den Absender als unzustellbar zurück schicken oder einem bestimmten Konto bzw. einem bestimmten Verteiler (Gruppe) zukommen lassen. Setzen Sie den Optionsschalter entsprechend und tragen Sie sofern dies erwünscht ist den lokalen Empfänger ein (Kontoname oder Gruppenname). Die Eingabe einer kompletten Mail-Adresse (mit @domain) ist hier nicht erlaubt.

Mit welcher Domain der DEFENDO selbst seine Mails verschickt, kann mit der Option „DEFENDO eMails erhalten die Domain“ festgelegt werden. Dieser Wert wird aus den Grundeinstellungen bezogen, kann aber

auch selbst definiert werden, wenn der entsprechende Optionsschalter gedrückt ist. Im allgemeinen sollte der Haken bei „in den Envelope übernehmen“ aktiviert sein, damit sich der DEFENDO unter dem selben Namen meldet.

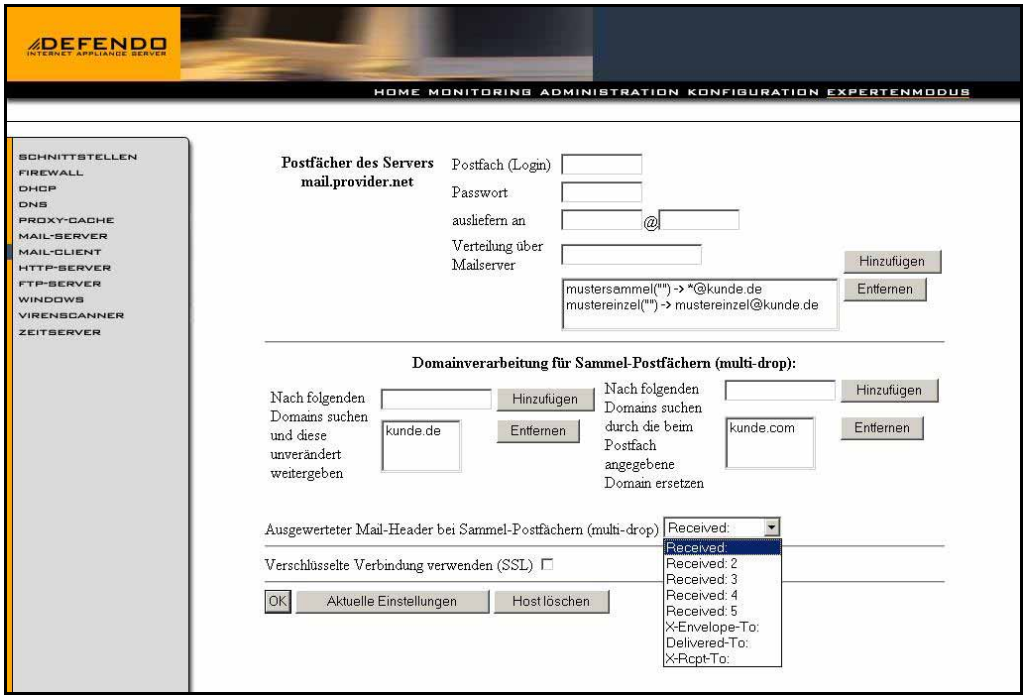
Wird eine ausgehende Mail nicht sofort versendet, so wird nach einer konfigurierbaren Zeitspanne eine Warnmeldung an den Absender generiert. Zu einer späteren Zeit wird die Mail als unzustellbar an den Absender zurückgeschickt. Bitte beachten Sie bei der Konfiguration dieser beiden Werte die zuvor eingestellten Versandzeitpunkte. So macht es z.B. keinen Sinn, bereits nach 1 Stunde eine Warnmeldung zu generieren, wenn ausgehende Mails gesammelt und alle 2 Stunden versendet werden.

Der Sinn einer Mail ist nicht die Übertragung von Datenmengen im Bereich von vielen Megabyte. Viele Mail-Server im Internet akzeptieren Mails nur bis zu einer bestimmten Größe oder brechen die Übertragung nach einer bestimmten Zeit ab. Es empfiehlt sich daher, eine entsprechende Beschränkung der Größe von Mails im SMTP-Server des DEFENDO. Bitte beachten Sie, daß diese Beschränkung sowohl für eingehende Mails als auch für ausgehende Mails gilt.

Drücken Sie auf „Übernehmen“ um Änderungen in der Konfiguration zu aktivieren oder „Aktuelle Einstellungen“ um noch nicht aktivierte Änderungen rückgängig zu machen.

12.7. Mail-Client

Über diese Funktion können Einstellungen für die Mail-Abholung gemacht werden. Soll der DEFENDO Mails von POP3-Servern im Internet abholen oder mit dem ESMTP ETRN-Befehl abrufen, so können Sie hier die entsprechenden Einstellungen vornehmen. Aufgrund der erforderlichen Abstimmung von Mail-Client und Mail-Server empfielt es sich die Abholung von POP3-Servern mit Hilfe des entsprechenden Konfigurations-Assistenten aus dem Assistenten-Menü vorzunehmen. Der Mail-Abruf von ETRN-Server ist über den Konfigurations-Assistenten nicht konfigurierbar.



Im Listenfeld unterhalb von „Mail abholen von folgenden Servern“ ist bereits in der Regel mindestens ein Eintrag hinterlegt, der durch den Konfigurations-Assistenten „eMail-Einrichtung“ übernommen wurde. Sie können jedoch hier weitere hinzufügen oder bestehende Einträge bearbeiten. Zum Bearbeiten selektieren Sie diesen bitte und wählen den Schalter „Bearbeiten“. Der DEFENDO wechselt daraufhin je nach Servertyp in die Bearbeitungsmaske für POP3- bzw. ETRN-Server (siehe Kapitel 12.7.1 bzw. 12.7.2). Sollten Sie neue Einträge hinzufügen wollen, tragen Sie diese bitte im Feld „Mail abholen von folgenden Servern“ den entsprechenden Hostnamen bzw. IP-Adresse ein und wählen den entsprechenden Servertyp im Listenfeld daneben aus. Klicken Sie auf den Schalter „Hinzufügen“. Der DEFENDO wechselt nun in die Bearbeitungsmaske des neuen Eintrages. Wollen Sie Einträge löschen, so ist vorher in die Bearbeitungsmaske zu wechseln.

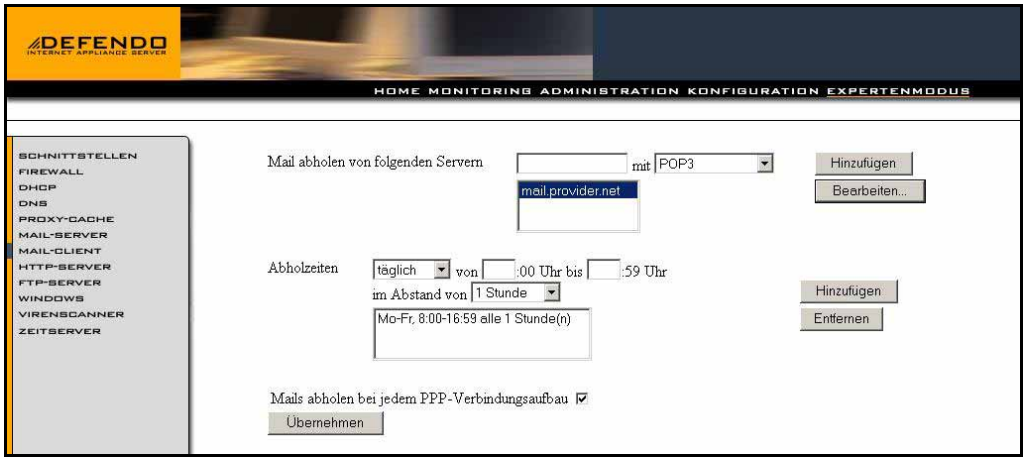
Im unteren Seitenbereich werden die Abholzeiten für eMails eingetragen. Auch hier sind ggf. durch die Konfiguration über den Konfigurations-Assistenten „eMail-Einrichtung“ bereits Werte hinterlegt. Ergänzen Sie oder entfernen Sie Einträge mit Hilfe der Schalter „Hinzufügen“ bzw. löschen. Sind keine POP3- oder ETRN-Server konfiguriert, so erfolgt zu den Konfigurierten Zeiten kein Verbindungsaufbau.

Wenn Sie mit einer PPP-Wählleitung an das Internet angebunden sind, kann zusätzlich zu den fest eingestellten Zeiten bei jedem Verbindungsaufbau ins Internet auf neue eMails geprüft werden. Aktivieren

Sie dazu bitte den Optionshaken bei „Mails abholen bei jedem Verbindungsaufbau“. Drücken Sie auf Übernehmen um Änderungen dieser Einstellung zu aktivieren.

12.7.1. Mail-Client Einträge bearbeiten (POP3)

Alle Einstellungen bezüglich Ihrer Postfächer bei Ihrem Provider sind hier hinterlegt. Das sind die Daten, die Sie von Ihrem Provider zur Verfügung gestellt bekommen, wie z. B. Postfachname, Benutzer und Passwort.



Alle angelegten Konten werden Ihnen im unteren Bereich im Listenfeld angezeigt. Fügen Sie neue hinzu, indem Sie die entsprechenden Felder mit den Daten Ihres Providers ausfüllen und über den Schalter „Hinzufügen“ bestätigen. Wählen Sie einen Eintrag im Listenfeld, um bestehende Konten zu entfernen. Als Wert „Postfach“ tragen Sie bitte den Benutzernamen für das entsprechende Konto auf dem POP3-Server des Providers ein. Diesen Wert sowie das zugehörige „Passwort“ erhalten Sie von Ihrem Provider. Tragen Sie bei „ausliefern an“ den lokalen Mail-Empfänger gefolgt von der gewünschten lokalen Domain ein. Wenn Sie keinen lokalen Empfänger eingeben, wird dieses Postfach als Sammelpostfach (Multi-Drop) abgefragt. Wenn Sie keine lokale Domain eingeben wird localhost angenommen. Wenn die Mail nicht an den Mail-Server des DEFENDO sondern an einen anderen SMTP-Mail-Server zugestellt werden soll, tragen Sie bitte dessen IP-Adresse bei „Verteilung über Mail-Server“ ein. Drücken Sie dann auf Hinzufügen.

Achtung:

Wird die Mail nicht über den Mail-Server des DEFENDO sondern direkt an einen internen Mail-Server weitergeleitet, so werden damit alle Funktionen und Sicherheitsmechanismen des DEFENDO Mail-Servers umgangen (Virenscan, Attachment-Filter, ...)

Konten werden in folgendem Format angezeigt, wobei die Angabe der Domain und des internen Mail-Servers fehlen kann:

Einzelkonto:

Kontoname („*Paßwort*“)->*Empfänger@domain* [smtp://*interner Server*]

Sammelkonto:

Kontoname („*Paßwort*“)- >**@domain* [smtp://*interner Server*]

Wählen Sie ein Postfach aus der Liste aus und drücken Sie auf Entfernen um ein Konto zu löschen. Sind keine Konten angegeben, so wird dieser POP3-Server nicht abgerufen.

Der folgende Bereich der Maske ist ausschließlich zur Konfiguration von Sammelpostfächern (Multi-Drop) notwendig. Sofern Sie von Ihrem Provider keine Sammelkonten abholen, muß hier nichts eingerichtet werden.

Bei einem Sammelpostfach laufen mehrere Mails in ein Konto (z.B. für die komplette eigene Mail-Domain). Dies hat den Vorteil, daß die Mail-Administration trotz POP3-Verfahrens lokal vorgenommen werden kann. Unter bestimmten Umständen kann es jedoch bei diesem Verfahren zu Fehlzustellungen kommen (insbesondere bei einigen Mailing-Listen oder Mail die als blinde Kopie Bcc geschickt wurde). Bei Abholung der Mail werden die Adreßinformationen der Mails durch den DEFENDO analysiert, um den tatsächlichen Empfänger zu ermitteln. Dazu müssen hier die Domains angegeben werden, nach denen in den Adreßinformationen gesucht werden soll um den Empfänger zu ermitteln. Es sind dabei zwei Möglichkeiten vorgesehen: Wenn die gefundene Adresse übernommen werden soll, tragen Sie die Domain im Bereich „Nach folgenden Domains suchen und unverändert weitergeben“ ein. Ist dort z.B. die Domain kunde.com eingetragen, so wird eine Mail an benutzer@kunde.com auch lokal an benutzer@kunde.com zugestellt. Der lokale Mail-Server muß in diesem Fall Mails an diese Domain annehmen. Wollen Sie Domaininformation hingegen verändern, so tragen Sie die zu suchende Domain im Feld „Nach folgenden Domains suchen und durch die beim Postfach angegebene Domain ersetzen“

ein. Wird z.B. provider.com eingetragen und beim Postfach kunde.com hinterlegt, so werden Mails an kunde@provider.com lokal an kunde@kunde.com zugestellt.

Wird in den Adreßdaten einer Mail keine der hier konfigurierten Domains gefunden, so wird die Mail an den Administrator zugestellt. Wurden keine Domains eingetragen, so gehen alle Mails aus dem Sammelpostfach an den Administrator.

Bei Sammelkonten wird nach den Domains normalerweise im ersten (aktuellsten) Received-Header der Mail gesucht. Sollten alle eingehenden Mails an den Administrator zugestellt werden obwohl die zu suchenden Domains hinterlegt wurden, ist die relevante Information möglicherweise in einem anderen Header zu finden. Dies lässt sich über die Einstellung „Ausgewerteter Mail-Header bei Sammel-Postfächern (multi-drop)“ konfigurieren. Wählen Sie z.B. „Received: 2“ wenn die Empfängeradresse im zweiten Received-Header vermerkt ist oder einen der anderen zur Auswahl stehenden Header aus. Bitte beachten Sie, dass der Mail-Client des DEFENDO ebenfalls einen Received-Header in die Mail einfügt. Das gleiche gilt für den Mail-Server des DEFENDO und / oder interne Mail-Server. Wenn Sie also die Mail-Header mit Hilfe Ihres Mail-Programmes inspizieren, sind alle Received-Header bis einschließlich des Received-Headers von „fetchmail“ zu entfernen. Ein Beispiel wie die Mail-Header in Ihrem Mail-Programm angezeigt werden könnten:

```
Received: from 192.168.0.254
        by interner.mail.server
        for <postmaster@kunde.com>
Received: from pop.provider.com
        by fetchmail POP3
        for <postmaster/kunde.com> (multi-drop)
Received: by pop.provider.com
        for kundenkonto
Received: from mail.absender.com
        by mail.provider.com
        for  <benutzer@kunde.com>
X-Envelope-To: benutzer@kunde.com
Received: from absender
        by mail.absender.com
        for <benutzer@kunde.com>
From: "Absender" <absender@absender.com>
To: benutzer@kunde.com
Subject: test
```

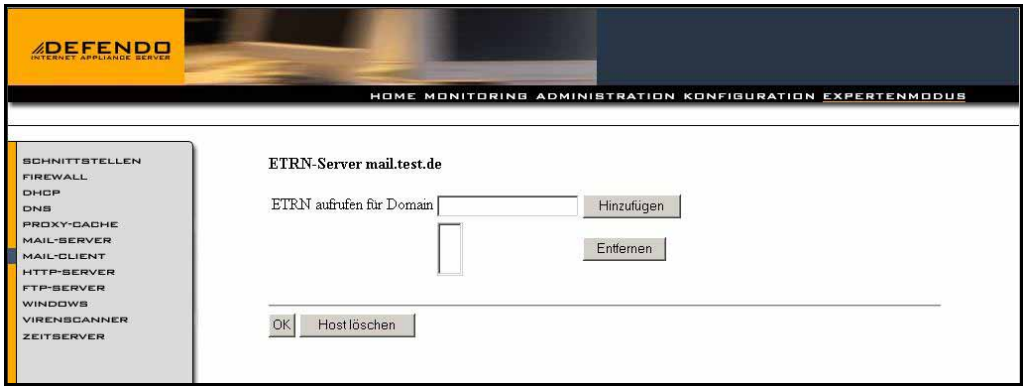
Der erste Received-Header im Beispiel ist vom internen Mail-Server erzeugt worden nachdem der DEFENDO die Mail an den internen Server ausgeliefert hat. Dieser Header wurde also nach der Abholung erzeugt und ist daher irrelevant. Der zweite Received-Header wurde vom Mail-Client „fetchmail“ des DEFENDO erzeugt und zeigt, dass das zugehörige Provider-Konto im multi-drop-Modus abgerufen wurde. Die Mail wird an postmaster@kunde.com zugestellt, da offensichtlich der korrekte Empfänger (benutzer@kunde.com) nicht erkannt wurde. Auch dieser Mail-Header ist zu ignorieren, da dieser erst durch den Mail-Client selbst erzeugt wurde, beim Abrufen aus dem POP-Konto des Providers also noch nicht vorhanden war. Standardmäßig wird also der unmittelbar darauf folgende Received-Header bei der Abholung des multi-drop-Kontos ausgewertet. Zum Zeitpunkt der Abholung aus dem POP-Konto des Providers ist dieser nämlich der erste Received-Header. Als Empfänger steht im obigen Beispiel lediglich „kundenkonto“, weswegen die Mail-Verteilung anhand dieses Headers fehlschlägt. Hier fehlt nämlich die Kundendomain nach der gesucht werden soll. Im Beispiel handelt es sich vielmehr lediglich um eine Providerinterne Umleitung der Mail. Im darauf folgenden Header steht dann aber zum ersten Mal der korrekte Empfänger. In der Oberfläche wäre folglich „Received: 2“ als ausgewerteter Mail-Header zu konfigurieren. Alternativ steht auch der „X-Envelope-To“-Header zur Verfügung. Dieser ist in der Regel noch zuverlässiger als ein Received-Header, jedoch in der Praxis eher selten vorhanden. Für das obige Beispiel wäre als „X-Envelope-To“ die beste Wahl für den ausgewerteten Mail-Header.

Bietet der Provider den SSL-verschlüsselten Zugriff auf seinen POP3-Server (TCP-Port 995) an, so kann dies mit dem entsprechenden Schalter aktiviert werden.

Zum Löschen des kompletten POP3-Servers mitsamt aller Einträge verwenden Sie bitte den Schalter „Host Löschen“. Eine entsprechende Sicherheitsabfrage muß hierfür bestätigt werden.

12.7.2. Mail-Client Einträge bearbeiten (ETRN)

In dieser Maske können Sie konfigurieren, welche Domains mit Hilfe des ESMTP-Befehls ETRN vom Mail-Server des Providers abgerufen werden sollen. Tragen Sie eine Domain ein und drücken Sie auf Hinzufügen um eine neue Domain aufzunehmen. Wählen Sie eine Domain aus und drücken Sie auf Entfernen um eine Domain zu löschen. Wenn keine Domain eingetragen ist erfolgt auch kein Verbindungsaufbau zum Mail-Server des Providers.



Bitte beachten Sie, daß bei ETRN die abgerufenen Mails vom Mail-Server des Providers mit dem SMTP-Protokoll zugestellt werden. Die Firewall-Konfiguration des DEFENDO ist für diesen Fall im allgemeinen anzupassen. Eingehende Verbindungen an den SMTP-Port des DEFENDO müssen vom Mail-Server des Providers aus akzeptiert werden.

Zum Löschen des kompletten ETRN-Servers mitsamt aller Einträge verwenden Sie bitte den Schalter „Host Löschen“. Eine entsprechende Sicherheitsabfrage muß hierfür bestätigt werden.

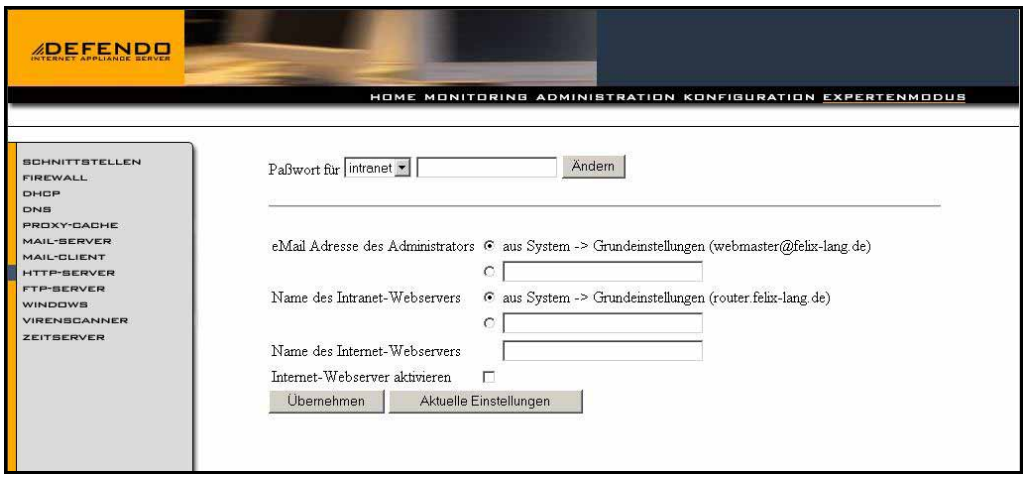
12.8. Http-Server

Der DEFENDO bietet Ihnen die Möglichkeit, Web-Seiten im Intranet und im Internet zu publizieren. Der Intranet-Bereich darf ausschließlich von den in den Grundeinstellungen als lokale Netzwerke hinterlegten IP-Adresse aus angesprochen werden. Die Verwaltung der Seiten ist sowohl über die Windows-Netzwerkumgebung als auch über ftp möglich. Der Zugriff auf das entsprechende Verzeichnis ist mit dem Login intranet möglich.

Der Zugriff auf den Internet-Web-Server ist von allen IP-Adressen aus möglich (sofern im Firewall freigeschalten). Die Verwaltung erfolgt ebenfalls über Windows-Netzwerkumgebung oder ftp mit dem Login www.

Beim Zugriff über ftp befinden Sie sich je nach FTP-Client bereits im Verzeichnis für die statischen Web-Seiten oder Sie befinden sich noch im Hauptverzeichnis. Vom Hauptverzeichnis aus werden statische Inhalte im Verzeichnis html abgelegt, dynamische Seiten werden durch Programme im Verzeichnis cgi-bin generiert. Der Aufruf von Programmen aus dem cgi-bin-Verzeichnis erfolgt über den Link http://Servername/cgi-bin/Programmname. Um zu verhindern, daß bei

statischen Seiten anstelle einer Verzeichnisliste eine bestimmte Seite angezeigt wird, muß diese entweder index.html oder index.htm genannt werden. Bitte beachten Sie bei der Verknüpfung von Dateien, daß bei Dateinamen Groß- und Kleinschreibung unterschieden wird.



Wählen Sie aus der Auswahlliste bei “Paßwort für” den Benutzer intranet oder www aus, tragen Sie das gewünschte Paßwort ein und drücken Sie auf Ändern. Das ftp- und Windows-Paßwort des ausgewählten Benutzers wird damit geändert.

Verwenden Sie die Mail-Adresse des Administrators aus den Grundeinstellungen oder aktivieren Sie das Optionsfeld vor dem Eingabebereich und tragen Sie dort selbst eine Mail-Adresse ein. Bei Fehlermeldungen im Browser wird dem Anwender diese Adresse als Kontaktadresse für den Web-Server angezeigt.

Verwenden Sie den Servernamen aus den Grundeinstellungen des DEFENDO oder aktivieren Sie das Optionsfeld vor dem Eingabebereich und tragen Sie selbst einen Server-Namen für den Intranet-Web-Server ein. Wenn Sie den Servernamen selbst vergeben müssen Sie außerdem für einen passenden DNS-Eintrag sorgen, der diesen Servernamen auf die LAN-IP-Adresse des DEFENDO abbildet. Der Intranet-Server hört auf den hier konfigurierten Namen oder auf die LAN-IP-Adresse.

Geben Sie im Feld “Name des Internet-Webservers” den entsprechenden Namen ein (z.B. www.kunde.com). Bitte beachten Sie, daß auch für einen passenden DNS-Eintrag zu sorgen ist, um diesen Namen auf die Internet-IP-Adresse des DEFENDO abzubilden. Ein entsprechender

Eintrag wird im allgemeinen durch Ihren Provider vorgenommen. Aktivieren Sie dann den Internet-Server mit dem entsprechenden Haken.

Drücken Sie auf Übernehmen um Änderungen zu aktivieren.

12.9. FTP-Server

Der DEFENDO bietet Ihnen die Möglichkeit, mit Hilfe eines anonymous FTP-Servers Dateien bereitzustellen. Die Verwaltung dieser Dateien erfolgt über ftp mit Hilfe des Logins ftpadmin.

Tragen Sie bei “Paßwort für ftpadmin” das gewünschte Paßwort ein und drücken Sie auf Ändern. Das ftp-Paßwort des Benutzers ftpadmin wird so auf einen anderen Wert gesetzt.

Bei “Zugriff auf FTP-Server” können Sie konfigurieren, wer sich mit dem FTP-Server verbinden darf. Unterschieden werden dabei verschiedene Bereiche: Der Zugriff für die Benutzer admin, der Zugriff für die Benutzer ftpadmin, www und intranet zur Pflege der entsprechenden FTP- und Webserver-Verzeichnisse und der Zugriff für anonymes FTP. Die Verzeichnisse der Webserver und des anonymen FTP sind dabei speziell abgesichert, so dass der FTP-Client diese nicht verlassen kann. Mit Hilfe der Auswahllisten kann für jeden der drei Bereiche eingestellt werden, ob der Zugriff gesperrt ist, nur für die lokalen IP-Subnetze der Grundeinstellungen erlaubt sein soll oder ob sich beliebige Clients zum jeweiligen Bereich verbinden dürfen.

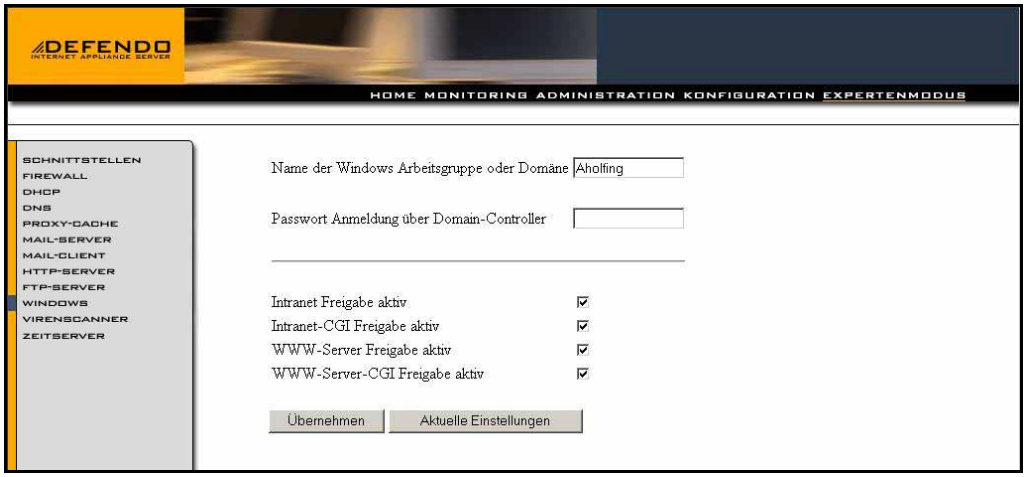
Wenn es möglich sein soll, bei anonymer Anmeldung Dateien auf dem DEFENDO zu speichern, aktivieren Sie bitte den entsprechenden Schalter. Die Dateien werden auf dem FTP-Server im Verzeichnis incoming abgelegt. Vom ftpadmin kann in diesem Verzeichnis eine maximal zweistufige Verzeichnishirarchie angelegt werden.

Für Fehlermeldungen können Sie die Mail-Adresse des Administrators aus den Grundeinstellungen übernehmen oder den Optionsschalter vor dem Eingabefeld aktivieren und selbst eine Mail-Adresse eintragen.

Drücken Sie auf Übernehmen um Änderungen in der Konfiguration zu aktivieren.

12.10. Windows

Die Windows-Freigaben des DEFENDO können verwendet werden um die Web-Server des DEFENDO bequem über die Windows-Netzwerkumgebung zu verwalten.



Bitte tragen Sie den Namen Ihrer Windows Arbeitsgruppe oder Domäne im entsprechenden Feld ein. Achtung: Verwechseln Sie bitte die Windows-Domäne nicht mit Ihrer Internet-Domain.

Wenn die Paßwortvalidierung nicht vom DEFENDO selbst vorgenommen werden soll sondern von Ihrem Windows-Domain-Controller, so tragen Sie desse NETBIOS-Namen bitte in das entsprechende Feld ein. In diesem Falle müssen die Benutzer intranet bzw. www auf dem Win-

dows-Domain-Controller angelegt sein. Lassen Sie dieses Feld leer, wenn die Paßwörter durch DEFENDO selbst validiert werden sollen.

Wählen Sie die Freigaben aus, die in der Netzwerkumgebung aktiv sein sollen: Über die Intranet-Freigabe INTRANET werden die Web-Seiten des Intranet-Servers gepflegt. Die Intranet-CGI-Freigabe INTRACGI kann verwendet werden um CGI-Skripte auf dem Intranet-Server abzulegen. Entsprechendes gilt für den Internet-Server mit den Freigaben WWW und WWWCGI.

Drücken Sie auf Übernehmen um Änderungen der Konfiguration zu aktivieren.

12.11. Virenscanner

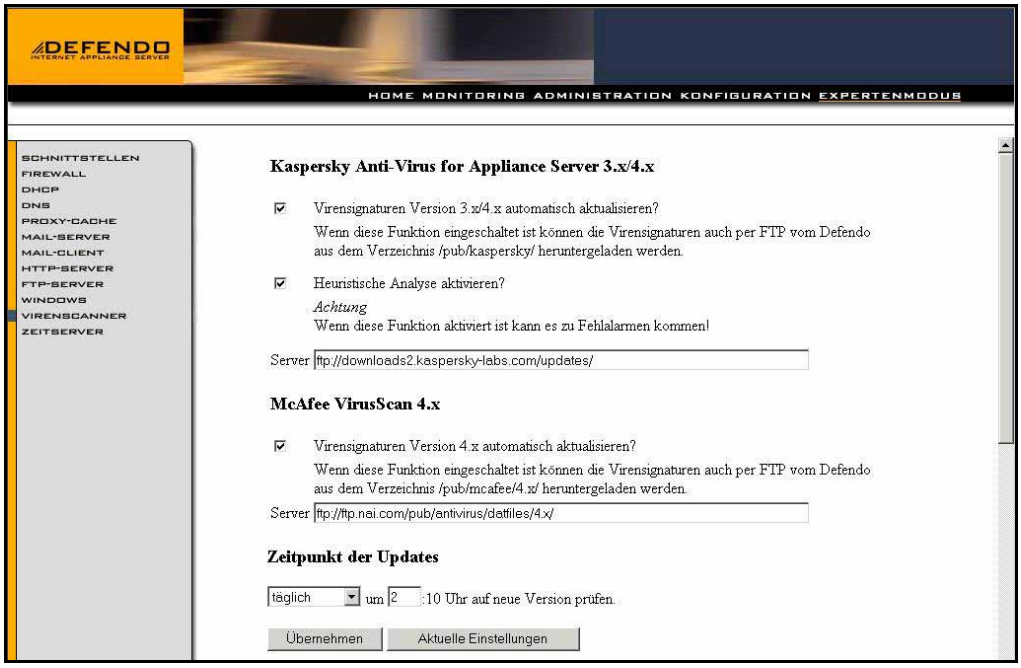
Der DEFENDO ist in der Lage, Virenschutzprogramme der Firma Kaspersky Lab Int. und der Firma McAfee einzusetzen.

Hinweis:

Zur Verwendung dieser Option ist der Erwerb der Virenscanner-Lizenz unbedingt notwendig. Die Lizenz ist im Lieferumfang nicht enthalten.

Von der Firma Kaspersky benötigen Sie das Produkt „Kaspersky Anti-Virus for Appliance Server 4.x“.

Für den Virenscan mit McAfee verwenden Sie bitte den Virenscanner für Linux Version 4.x aus einem der folgenden Produkte: „VirusScan Security Suite“, „Active VirusScan Security Suite“, „Total Virus Defense Suite“ oder „Active Virus Defense Suite“.



Die Aktualisierung der Signaturen im DEFENDO findet automatisch statt wenn Sie den Schalter „Virensignaturen Version x automatisch aktualisieren“ für den von Ihnen eingesetzten Virenscanner setzen. Im Feld „Server“ ist jeweils die Standard-Adresse eingetragen, über den Updates der Virensignaturen bezogen werden können. Dieser kann sich von Zeit zu Zeit ändern. Bitte vergewissern Sie sich in regelmäßigen Abständen über die Homepage des jeweiligen Herstellers, ob die hinterlegte Adresse noch gültig ist und ändern Sie den Eintrag wenn nötig entsprechend ab. Geben Sie die Adresse Grundsätzlich in URL-Schreibweise ein: ftp://Servername/Pfad. Sollte der Download nur über einen vorgeschalteten Proxy möglich sein, so fügen Sie bitte ein Leerzeichen und eine Proxy-Spezifikation an: proxy://Servername:Serverport. Erfordert der Proxy eine Benutzeranmeldung, so verwenden Sie bitte folgendes Format: proxy://Benutzerkennung:Passwort@Servername:Serverport. Sollte es sich bei dem Proxy um einen reinen ftp-Proxy handeln, so ersetzen Sie bitte proxy:// durch ftpproxy://.

Für den Kaspersky Virenscanner kann mit Hilfe des entsprechenden Schalters zusätzlich die heuristische Analyse aktiviert werden. Dabei werden gescannte Dateien nach bestimmten Mustern durchsucht, die für Viren typisch sind. So besteht die Chance, schädigende Inhalte zu erkennen auch wenn dafür noch keine Virenscanner-Signaturen bekannt oder installiert sind.

Über das Listenfeld können Sie die Wochentage sowie die Uhrzeit einstellen, wann der DEFENDO nach neuen Versionen von Virensignaturen schauen soll. Kaspersky Lab Int. aktualisiert täglich die Signaturen. Bei McAfee erfolgt die Aktualisierung in der Regel wöchentlich. Bitte beachten Sie hierzu auch die Informationen des Herstellers.

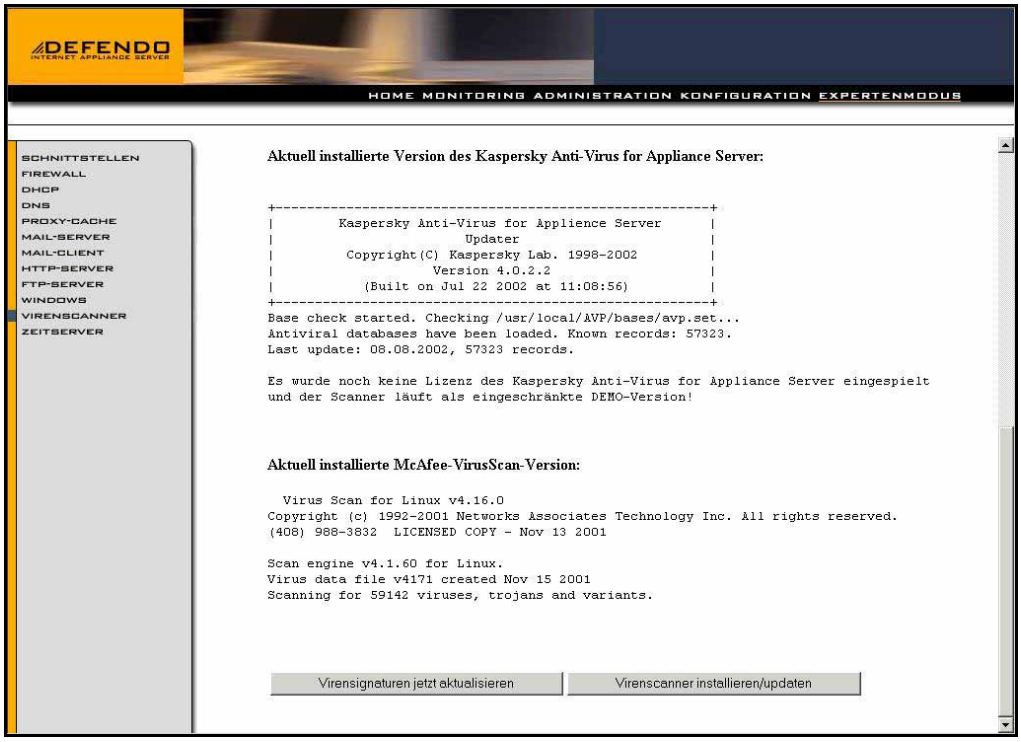
Achtung:

In unregelmäßigen Zeitabständen gibt es auch neue Versionen des Virenscanner-Programmes selbst. Das Herunterladen der neuesten Version des Programmes erfordert Ihre Lizenzdaten und kann daher nicht automatisch durchgeführt werden. Bitte prüfen Sie regelmäßig, ob aktuellere Version des Virenscanners angeboten werden. Mit veralteten Virenscan-Programmen werden möglicherweise nicht alle Viren erkannt, die in den Signaturen enthalten sind.

Um die neue Virensignatur auch anderen Servern oder PCs im Netz zugänglich zu machen, werden die Signaturdateien vom DEFENDO in der Verzeichnisstruktur des FTP-Servers abgelegt. Von dort können sie mit anonymous-FTP durch die Server oder PCs abgeholt werden. Die Kaspersky Signaturen befinden sich im Verzeichnis /pub/kaspersky/. McAfee Signaturen für Version 4.x finden Sie im Verzeichnis /pub/mcafee/4.x/.

Drücken Sie auf „Übernehmen“ um Änderungen an den Einstellungen zu aktivieren.

Im nächsten Bereich der Maske wird angezeigt, welche Virenscanner installiert sind und in welcher Version. Ferner wird hier auch der Stand der installierten Virensignaturen ersichtlich.



Drücken Sie auf „Virenscanner installieren / updaten“ um einen Virenscanner erstmalig zu installieren, zu erneuern oder um sie zu deinstallieren.

Achtung:

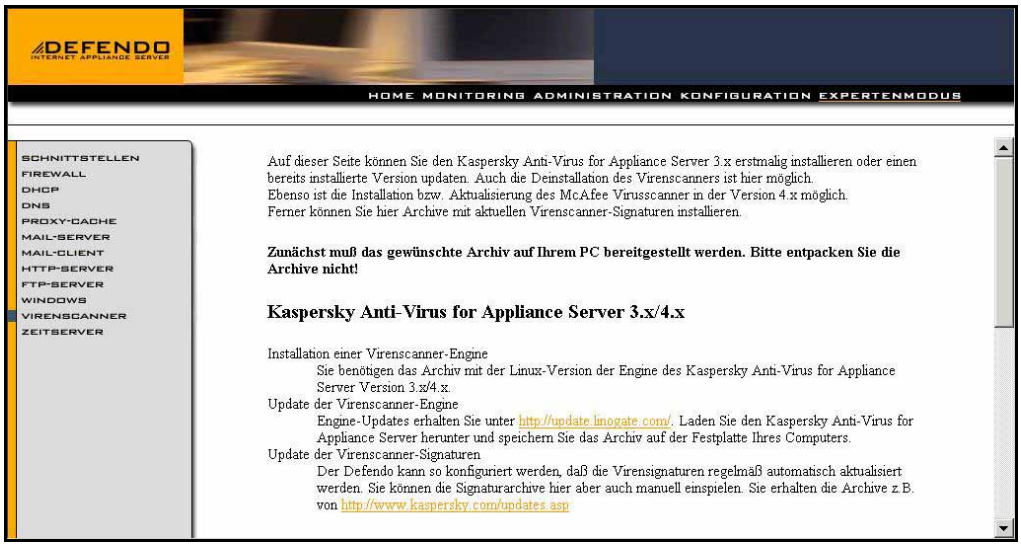
Das bloße Installieren des Virenscanners reicht nicht, um auch entsprechenden Virenschutz zu erhalten. Sie müssen die Virenüberprüfung für ihre eMail-Kommunikation (siehe Kapitel 12.6) und / oder die Virenüberprüfung des Proxy-Caches (siehe Kapitel 12.5) noch aktivieren.

Der Schalter „Virensignaturen jetzt aktualisieren“ ermöglicht es Ihnen, den sofortigen Download der aktuellen Virensignaturen zu starten. Es werden dabei jedoch nur die Signaturen der Virenscanner geladen, für die auch der automatische Download aktiviert ist. Insbesondere bei der ersten Aktualisierung werden dabei bis zu 10Mb Daten heruntergeladen. Bitte berücksichtigen Sie die dazu erforderliche Zeitdauer.

12.11.1. Installation Kaspersky Virenscanner

Wollen Sie einen neuen Virenscanner auf dem DEFENDO installieren oder eine aktuellere Version des Virenscanners einspielen, so gehen

Sie bitte wie folgt vor. Klicken Sie in der Grundmaske „Administration – Virenscanner“ auf den Schalter „Virenscanner installieren / updaten“. Der DEFENDO wechselt in die Installationsmaske:


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION EXPERTENMODUS
SCHNITTSTELLEN
FIREWALL
DHCP
DNS
PROXY-CACHE
MAIL-SERVER
MAIL-CLIENT
HTTP-SERVER
FTP-SERVER
WINDOWS
VIRENSCANNER
ZEITSERVER
Auf dieser Seite können Sie den Kaspersky Anti-Virus for Appliance Server 3.x erstmalig installieren oder einen bereits installierte Version updaten. Auch die Deinstallation des Virenscanners ist hier möglich.
Ebenso ist die Installation bzw. Aktualisierung des McAfee Virusscanner in der Version 4.x möglich.
Ferner können Sie hier Archive mit aktuellen Virenscanner-Signaturen installieren.
Zunächst muß das gewünschte Archiv auf Ihrem PC bereitgestellt werden. Bitte entpacken Sie die Archive nicht!
Kaspersky Anti-Virus for Appliance Server 3.x/4.x
Installation einer Virenscanner-Engine
Sie benötigen das Archiv mit der Linux-Version der Engine des Kaspersky Anti-Virus for Appliance Server Version 3.x/4.x.
Update der Virenscanner-Engine
Engine-Updates erhalten Sie unter http://update.linogate.com/. Laden Sie den Kaspersky Anti-Virus for Appliance Server herunter und speichern Sie das Archiv auf der Festplatte Ihres Computers.
Update der Virenscanner-Signaturen
Der Defendo kann so konfiguriert werden, daß die Virensignaturen regelmäß automatisch aktualisiert werden. Sie können die Signaturarchive hier aber auch manuell einspielen. Sie erhalten die Archive z.B. von http://www.kaspersky.com/updates.asp

Sie benötigen nun von Ihrem PC aus Zugriff auf ein Archiv mit dem „Kaspersky Anti-Virus for Appliance Server 4.x“. Bei der Erstinstallation und bei Erneuerung einer abgelaufenen Lizenz ist ferner eine Lizenzschlüssel-Datei mit .key als Dateiendung notwendig.

Updates der Virenscanner-Software erhalten Sie unter der Internetadresse www.linogate.de/update. Speichern Sie das Archiv auf der Festplatte Ihres Computers. Bitte entpacken Sie das Archiv nicht!

Das Archiv der Virenscanner-Software wird auf folgende Weise an den DEFENDO übermittelt: Drücken Sie hierzu den Schalter „Durchsuchen“. Wählen Sie bitte die entsprechende Installationsdatei auf Ihrer Festplatte an und drücken Sie auf „Öffnen“. Der Pfad zum Virenscanner-Archiv auf Ihrem PC ist nun in der Maske eingetragen. Mit „OK“ wird nun das Archiv übermittelt und dann der Virenscanner automatisch installiert. Bitte prüfen Sie nach ob in der Folgemaske der Virenscanner als installiert angezeigt wird.

Bei einer Erstinstallation und bei der Erneuerung einer abgelaufenen Lizenz muß auf gleiche Weise der Lizenzschlüssel eingespielt werden. Wählen Sie die entsprechende .key-Datei mit Hilfe des „Durchsuchen“-Dialoges aus und Übermitteln Sie diese mit „OK“. Bitte prüfen Sie nach ob in der Folgemaske der Virenscanner den Schlüssel als gültig akzeptiert hat.

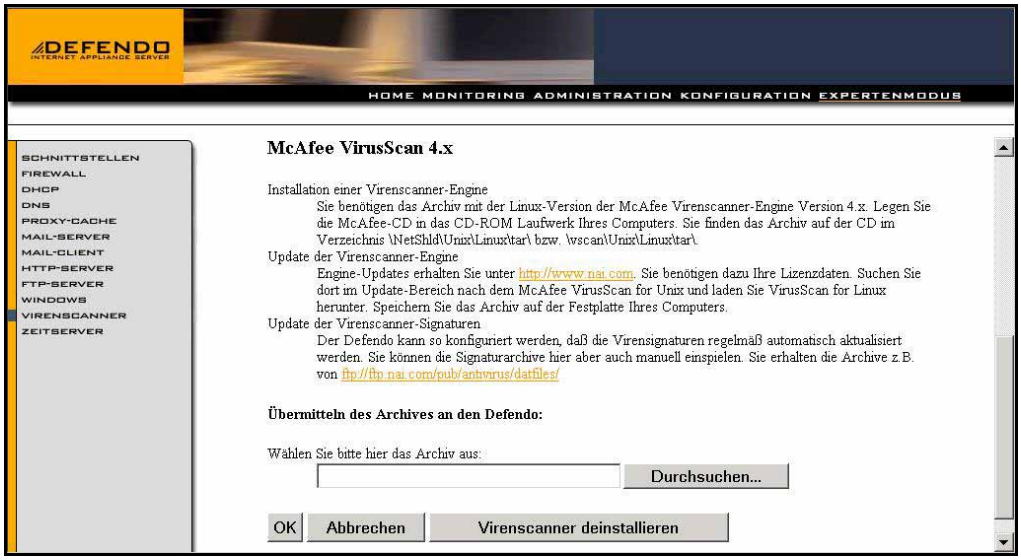
Auf die selbe Weise wie das Virenscanner-Programm können auch Virensignatur-Updates manuell eingespielt werden. Wählen Sie dazu mit

„Durchsuchen“ ein Signatur-Archiv und übermitteln Sie es wie zuvor beschrieben.

Zum Deinstallieren des Virenscanners drücken Sie bitte den entsprechenden Schalter.

12.11.2. Installation McAfee Virenscanner

Wollen Sie einen neuen Virenscanner auf dem DEFENDO installieren oder eine aktuellere Version des Virenscanners einspielen, so gehen Sie bitte wie folgt vor. Klicken Sie in der Grundmaske „Administration – Virenscanner“ auf den Schalter „Virenscanner installieren / updaten“. Der DEFENDO wechselt in die Installationsmaske:


DEFENDO
INTERNET APPLIANCE SERVER
HOME MONITORING ADMINISTRATION KONFIGURATION EXPERTENMODUS
SCHNITTSTELLEN
FIREWALL
DHCP
DNS
PROXY-CACHE
MAIL-SERVER
MAIL-CLIENT
HTTP-SERVER
FTP-SERVER
WINDOWS
VIRENSCANNER
ZEITSERVER
McAfee VirusScan 4.x
Installation einer Virenscanner-Engine
Sie benötigen das Archiv mit der Linux-Version der McAfee Virenscanner-Engine Version 4.x. Legen Sie die McAfee-CD in das CD-ROM Laufwerk Ihres Computers. Sie finden das Archiv auf der CD im Verzeichnis \NetShld\Unix\Linux\tar\ bzw. \vscan\Unix\Linux\tar\.
Update der Virenscanner-Engine
Engine-Updates erhalten Sie unter http://www.nai.com. Sie benötigen dazu Ihre Lizenzdaten. Suchen Sie dort im Update-Bereich nach dem McAfee VirusScan for Unix und laden Sie VirusScan for Linux herunter. Speichern Sie das Archiv auf der Festplatte Ihres Computers.
Update der Virenscanner-Signaturen
Der Defendo kann so konfiguriert werden, daß die Virensignaturen regelmäß automatisch aktualisiert werden. Sie können die Signaturarchive hier aber auch manuell einspielen. Sie erhalten die Archive z.B. von ftp://ftp.nai.com/pub/antivirus/datfiles/
Übermitteln des Archives an den Defendo:
Wählen Sie bitte hier das Archiv aus:
Durchsuchen...
OK
Abbrechen
Virenscanner deinstallieren

Sie benötigen nun von Ihrem PC aus Zugriff auf ein Archiv mit der Linux-Version der McAfee Virenscanner-Engine Version 4.x. Sie finden dieses auf der McAfee-CD im Verzeichnis \NetShield\Unix\Linux\tar oder \vcsan\Unix\Linux\tar

Updates erhalten Sie im Internet unter der Adresse http://www.nai.com oder http://www.mcafee.com. Zum Herunterladen eines Updates benötigen Sie Ihre Lizenzdaten. Suchen Sie im Update-Bereich nach dem McAfee VirusScan for Unix und laden Sie VirusScan for Linux herunter. Speichern Sie das Archiv auf der Festplatte Ihres Computers. Bitte entpacken Sie das Archiv nicht!

Das Archiv muß nun an den DEFENDO übermittelt werden. Verwenden Sie hierzu den Schalter „Durchsuchen“. Wählen Sie bitte die entsprechende Installationsdatei auf Ihrem CD-ROM-Laufwerk oder Ihrer Festplatte an und drücken Sie auf „Öffnen“. Der Pfad zum Virenscanner-Archiv auf Ihrem PC ist nun in der Maske eingetragen. Mit „OK“ wird nun das Archiv übermittelt und dann der Virenscanner automatisch installiert. Bitte prüfen Sie nach ob in der Folgemaske der Virenscanner als installiert angezeigt wird.

Auf die selbe Weise wie das Virenscanner-Programm können auch Virensignatur-Updates manuell eingespielt werden. Wählen Sie dazu mit „Durchsuchen“ ein Signatur-Archiv und übermitteln Sie es wie zuvor beschrieben.

Zum Deinstallieren des Virenscanners drücken Sie bitte den entsprechenden Schalter.

12.12. Zeit-Server

Der DEFENDO holt sich die genaue Uhrzeit über öffentliche Zeitserver im Internet. Diese sind bereits voreingestellt, können jedoch auch verändert oder andere neu hinzugefügt werden.

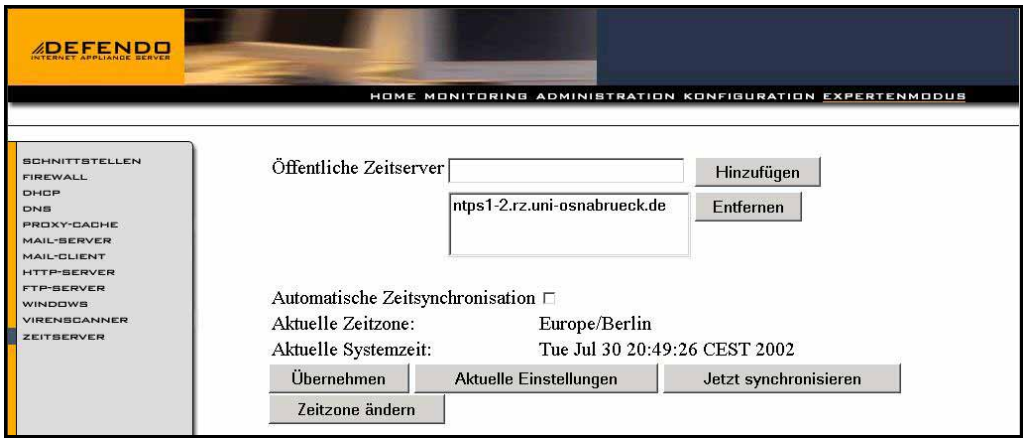
Mit dieser Funktion können Sie auch Ihre PCs oder andere Server im Netz mit der Atomzeit synchronisieren. Unter Windows 9.x oder Windows NT Betriebssystem ist es hierfür notwendig, das der DEFENDO - Dienst „Windows-Freigaben“ eingeschaltet ist (siehe Kapitel 12.10). Verwenden Sie den Befehl

NET TIME /SET \\< *IP-Adresse des* DEFENDO *oder Hostname> /YES*

z. B. im Login-Script Ihres NT-Servers oder einer Batch-Datei am PC selber. Bei jeder Abarbeitung des Scriptes oder der Batch-Datei wird die Uhrzeit des PCs mit der aktuellen Atomzeit synchronisiert.

Hinweis:

Sollten Sie Windows NT Workstation im Einsatz haben, so benötigt der Benutzer die entsprechenden Rechte die Uhrzeit des Systems zu ändern! Lesen Sie hierzu im Handbuch des Betriebssystems nach.



Über die Schalter „Hinzufügen“ und „Entfernen“ können entsprechend Zeitserver aufgenommen oder gelöscht werden. Die hier angegebenen Zeitserver müssen das time-Protokoll (TCP-Port 37) nach RFC 868 unterstützen.

Ist der Schalter „automatische Zeitsynchronisation“ aktiviert, synchronisiert der DEFENDO jeden Sonntag zwischen 4:00 Uhr und 4:59 Uhr seine Systemzeit mit den konfigurierten Zeitservern. Die zeitnahe Umstellung zwischen Sommer- und Winterzeit ist so gewährleistet.

Wollen Sie eine sofortige Synchronisation durchführen, bestätigen Sie den Schalter „Jetzt synchronisieren“. Bitte beachten Sie, dass für einen Abgleich eine Verbindung ist Internet notwendig ist.

Um die Zeitzone zu wechseln wählen Sie bitte die entsprechende Schaltfläche. In der folgenden Maske müssen Sie zunächst den gewünschten Kontinent auswählen. Fahren Sie fort mit „Weiter“. Wählen Sie in der nächsten Maske die Landeshauptstadt bzw. Region aus, deren Zeitzone eingestellt werden soll. Mit „Fertigstellen“ wird die neue Zeitzone aktiviert.

Alle Eingaben werden über den Schalter „Übernehmen“ im DEFENDO gespeichert. Sollten Sie sich nicht sicher sein, so können Sie die aktuellen Einstellungen über den Schalter „Aktuelle Werte“ zurückholen.

13. Kontakt

Wir sind stets bemüht, Ihnen bei jeglicher Art von Problemen zu helfen. Dafür haben Sie mehrere Möglichkeiten, mit uns Kontakt aufzunehmen.

Für Supportfragen wenden Sie sich bitte als erstes an Ihren Fachhändler. Sie finden eine Liste aller autorisierten Fachhändler im Internet unter www.linogate.de

Sie erreichen uns als Hersteller unter folgender Briefanschrift:

Linogate GmbH

Alter Postweg 101

86159 Augsburg

Wir sind im Internet sind wir unter folgenden WEB-Adressen erreichbar:

http://www.linogate.de/

http://www.defendo.de/

Wenn Sie uns per eMail erreichen wollen, so verwenden Sie bitte: support@linogate.de

14. Support für Ihren DEFENDO

Ein Online-Support (Fernwartung) Ihres Defendo kann nach Absprache mit Ihnen via RAS-Zugriff realisiert werden. Dies ist auch möglich, wenn Ihr Defendo keinen Zugriff zum Internet hat.

Weiteren Support wie eine umfangreiche Knowledge-Base sowie FAQs zu bekannten Fragen finden Sie im Internet unter:

http://www.linogate.de/support

Updates erhalten Sie unter der WWW-Adresse:

http://www.linogate.de/update

Für eine Anfrage halten Sie bitte folgende Informationen bereit:

Fernwartungs-IP-Adresse (siehe Kapitel 10.2)

Version und Updatelevel (siehe Kapitel 10.2)

Bei allgemeinen Problemen: Datum, Uhrzeit und wann das Problem aufgetreten ist mit einer möglichst detaillierten Fehlerbeschreibung.

Wenn Sie eine Fehlermeldung erhalten haben: Datum und Uhrzeit der Fehlermeldung sowie der genaue Wortlaut der Fehlermeldung.

15. Technische Daten

Hinweis:

Alle technischen Werte können je nach Ausstattung unterschiedlich sein.

Gehäuseabmessung:	Desktop: 324 mm / 374 mm / 93 mm
	19": 1 HE, 430 tief
Gewicht:	ca. 7 kg
Ethernetanschluß:	10/100 Mbit 10-BaseT/100-BaseTX, RJ45
ISDN-Adapter :	ELSA Microlink ISDN
Schnittstellen :	2 x 9 pol. RS-232 Schnittstelle
Prozessor:	mind. Intel Celeron 1 GHz
Speicher:	mind. 128 MB RAM
Festplatte:	E-IDE mit mind. 10 Gbyte Kapazität
Leistungsaufnahme:	< 50 Watt
Zulassungen:	EN 60950, UL 1950, VDE 0805

16. CE-Konfirmitätserklärung

Der DEFENDO erfüllt in der ausgelieferten Ausführung die Anforderungen der EG-Richlinien 89/336/EWG "Elektromagnetischer Verträglichkeit" und 73/23/EWG "Niederspannungsrichtlinie".